

10/049264

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 5 月 16 日 (16.05.2002)

PCT

(10) 国際公開番号
WO 02/39664 A2

- (51) 国際特許分類: H04L 9/30, G09C 1/00 (OKEYA, Katsuyuki) [JP/JP]; 〒244-0003 神奈川県横浜市戸塚区戸塚町5030番地 株式会社 日立製作所 ソフトウェア事業部内 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP01/09781
- (22) 国際出願日: 2001 年 11 月 8 日 (08.11.2001) (74) 代理人: 浅村 皓, 外(ASAMURA, Kiyoshi et al.); 〒100-0004 東京都千代田区大手町2丁目2番1号 新大手町ビル331 Tokyo (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語 (81) 指定国 (国内): US.
- (30) 優先権データ: 特願2000-345457 2000 年 11 月 8 日 (08.11.2000) JP (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
特願 2000-393279 2000 年 12 月 21 日 (21.12.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 桶屋勝幸
- 添付公開書類:
— 第17条(2)(a)に基づく宣言; 要約なし; 国際調査機関により点検されていない発明の名称。
- 2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。



WO 02/39664 A2

(54) Title: ELLIPTIC CURVE SCALAR MULTIPLE CALCULATION METHOD AND DEVICE, AND STORAGE MEDIUM

(54) 発明の名称: 楕円曲線スカラー倍計算方法及び装置並びに記憶媒体

(57) Abstract:



明 細 書

楕円曲線スカラー倍計算方法及び装置並びに記憶媒体

5 技術分野

本発明はコンピュータネットワークにおけるセキュリティ技術に係り、特に楕円曲線暗号における暗号処理実行方法に関する。

背景技術

- 楕円曲線暗号はN. Koblitz, V. S. Millerにより提案された公開鍵暗号の一種である。公開鍵暗号には、公開鍵と呼ばれる一般に公開してよい情報と、秘密鍵と呼ばれる秘匿しなければならない秘密情報がある。与えられたメッセージの暗号化や署名の検証には公開鍵を用い、与えられたメッセージの復号化や署名の作成には秘密鍵を用いる。楕円曲線暗号における秘密鍵は、スカラー値が担っている。また、楕円曲線暗号の安全性は楕円曲線上の離散対数問題の求解が困難であること
- 10 15 20 25
- とに由来している。ここで楕円曲線上の離散対数問題とは、楕円曲線上のある点Pとそのスカラー倍の点dPが与えられた時、スカラー値dを求める問題である。ここにおいて、楕円曲線上の点とは、楕円曲線の定義方程式をみたす数の組をいい、楕円曲線上の点全体には、無限遠点という仮想的な点を単位元とした演算、すなわち楕円曲線上の加法（乃至は加算）が定義される。そして、同じ点同士の楕円曲線上の加法のことを、特に楕円曲線上の2倍算という。楕円曲線上の2点の加法は次のようにして計算される。2点を通る直線を引くとその直線は楕円曲線と他の点において交わる。その交わった点とx軸に関して対称な点を加法を行なった結果の点とする。楕円曲線上の点の2倍算は次のようにして計算される。楕円曲線上の点における接線をひくと、その接線は楕円曲線上の他の点において交わる。その交わった点とx座標に関して対称な点を2倍算を行なった結果の点とする。ある点に対し、特定の回数だけ加法を行なうことをスカラー倍といい、その結果をスカラー倍点、その回数のことをスカラー値という。

情報通信ネットワークの進展と共に電子情報に対する秘匿や認証の為に暗号技術は不可欠な要素となってきている。そこでは暗号技術の安全性とともに高速化

が望まれている。楕円曲線上の離散対数問題が非常に困難である為に、素因数分解の困難性を安全性の根拠にしているRSA暗号と比べて、楕円曲線暗号は鍵長を比較的短くすることができる。そのため比較的高速な暗号処理が可能である。

しかしながら、処理能力の制限されているスマートカードや大量の暗号処理を行なう必要のあるサーバ等においては、必ずしも満足できる程高速であるとは限らない。それゆえに暗号のさらなる高速化が必要となる。

楕円曲線暗号には、ワイエルシュトラス型楕円曲線と呼ばれる楕円曲線が通常用いられている。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology proceedings of ASIACRYPT'98, LNCS 1514, Springer-Verlag, (1998) pp. 51-65

10 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この計算方法は、スカラー倍点の座標を、省略することなく正確に表示している。すなわち、アフィン座標系であれば、x座標

15 及びy座標、射影座標乃至はヤコビアン座標であれば、X座標、Y座標及びZ座標の値を全て与えている。

一方でモンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ ($A, B \in F_p$) を用いるとワイエルシュトラス型楕円曲線よりも高速に演算を実行できることが

P. L. Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization, Math. Comp. 48 (1987) pp. 243-264. に記載されている。これ

20 は、スカラー値の特定のビットの値に依存して、楕円曲線上の点の組 $(mP, (m+1)P)$ から点の組 $(2mP, (2m+1)P)$ 乃至は点の組 $((2m+1)P, (2m+2)P)$ を繰り返して計算するスカラー倍計算方法において、モンゴメリ型楕円曲線を利用することにより、加算及び2倍算の計算時間が短縮されることに由来する。このスカラー

25 倍計算方法は、ワイエルシュトラス型楕円曲線における、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いた場合よりも、高速に計算することができる。しかしながら、この方法は楕円曲線上の点のy座標の値は計算しない。多くの暗号処理においては、本質的にy座標を用いないので、この事は問題にはならないが、一部の暗号処理を実行する又は完全な形で標準に準拠しようとすれ

ば、 y 座標の値も必要となる。

以上は楕円曲線の定義体の標数が5以上の素数の場合であるが、他方、標数2の有限体上定義された楕円曲線に対しては、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法が J. Lopez, R. Dahab, Fast Multiplication on

- 5 Elliptic Curves over $GF(2^m)$ without Precomputation, Cryptographics Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp.316-327. に記載されている。

- 上記従来技術により、標数が5以上の有限体上定義された楕円曲線を用いて楕円曲線暗号を構成した場合、ワイエルシュトラス型楕円曲線においてウィンドウ法及び混合座標系を用いると、スカラー倍点の座標を完全に計算することができるが、モンゴメリ型楕円曲線のスカラー倍計算方法を用いた場合程高速に計算することはできない。モンゴメリ型楕円曲線におけるスカラー倍計算方法を用いると、ワイエルシュトラス型楕円曲線においてウィンドウ法及び混合座標系を用いた場合より高速に計算することが可能であるが、スカラー倍点の座標を完全に与えること、すなわち y 座標を計算することができない。したがって、スカラー倍計算方法として、高速化を計ろうとするとスカラー倍点の座標を完全に与えることができず、スカラー倍点の座標を完全に与えようとする高速に計算ができないという状態にあった。
- 15

発明の開示

- 20 本発明の目的は、標数が5以上の有限体上定義された楕円曲線において、モンゴメリ型楕円曲線におけるスカラー倍演算と同程度の高速さで、スカラー倍点の座標を完全に与えることができる、即ち、 x 座標と y 座標を共に計算できるスカラー倍計算方法を提供することにある。

- 上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有することを特徴とする。
- 25

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限

体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報からアフィン座標において完全な座標を復元するステップとを有することを特徴とする。

- 5 また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から射影座標において完全な座標を復元するステップとを有することを特徴とする。
- 10 また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有することを特徴とする。
- 15 また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有することを特徴とする。
- 20 また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点の X 座標及び Z 座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標における X 座標及び Z 座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。
- 25 また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円

円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点のx座標、前記スカラー倍点と前

記モンゴメリ型楕円曲線上の点を加算した点のアフィン座標における x 座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点のアフィン座標における x 座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

- 5 また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点の X 座標及び Z 座標、
- 10 前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標における X 座標及び Z 座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標における X 座標及び Z 座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。
- 15 また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点の X 座標及び Z 座標、
- 20 前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標における X 座標及び Z 座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標における X 座標及び Z 座標を与え、射影座標において完全な座標を復元するステップとを有することを特徴とする。

- また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限
- 25 体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点の x 座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点のアフィ

ン座標における x 座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点のアフィン座標における x 座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

- また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限
- 5 体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報から
- 10 ワイエルシュトラス型楕円曲線において完全な座標を復元するステップとを有することを特徴とする。

- また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法
- 15 であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からモンゴメリ型楕円曲線において完全な座標を復元するステップと、前記モンゴメリ型楕円曲線において完全な座標が復元されたスカラー倍点からワイエルシュト
- 20 ラス型楕円曲線におけるスカラー倍点を計算するステップとを有することを特徴とする。

- また上記目的を達する一手段として、楕円曲線暗号における標数 5 以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法
- 25 であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点の X 座標及び Z 座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の

射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有することを特徴とする。

- また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限
- 5 上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報として
- 10 モンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有することを特徴とする。

- また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限
- 15 体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報として
- 20 てモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップ
- 25 とを含むことを特徴とする。

また本発明は、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴ

メリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線においてアフィン座標で与えられたスカラー倍点のx座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点のアフィン座標におけるx座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点のアフィン座標におけるx座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有することを特徴とする。

図面の簡単な説明

図1は本発明の暗号処理システムの構成図である。

図2は本発明の実施例におけるスカラー倍計算方法及び装置における処理の流れを示す図である。

図3は図1の暗号処理システムでの処理の流れを示すシーケンス図である。

図4は本発明の第1、第2、第14及び第15実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図5は本発明の第3及び第4実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図6は本発明の第5実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図7は本発明の第6、第7及び第8実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

- 5 図8は本発明の第9、第10、第20及び第21実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図9は本発明の第2実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

- 10 図10は本発明の第11及び第12実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図11は本発明の第1実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図12は本発明の第3実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

- 15 図13は本発明の第4実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図14は本発明の第6実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

- 20 図15は本発明の第7実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図16は本発明の第8実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図17は本発明の第9実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

- 25 図18は本発明の第10実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図19は本発明の第11実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図20は本発明の第12実施例のスカラー倍計算方法における座標復元方法を

示すフローチャート図である。

図 2 1 は本発明の第 1 3 実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図 2 2 は本発明の実施の形態に係る署名作成装置の構成図である。

- 5 図 2 3 は本発明の実施の形態に係る復号化装置の構成図である。

図 2 4 は本発明の第 1 3 実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図 2 5 は図 2 のスカラー倍計算部におけるスカラー倍計算方法を示すフローチャートである。

- 10 図 2 6 は本発明の第 5 実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図 2 7 は本発明の実施例におけるスカラー倍計算方法及び装置における処理の流れを示す図である。

- 15 図 2 8 は図 2 2 の署名作成装置における署名作成方法を示すフローチャートである。

図 2 9 は図 2 2 の署名作成装置における処理の流れを示すシーケンス図である。

図 3 0 は図 2 3 の復号化装置における復号化方法を示すフローチャートである。

図 3 1 は図 2 3 の復号化装置における処理の流れを示すシーケンス図である。

- 20 図 3 2 は図 1 の暗号処理システムにおける暗号処理方法を示すフローチャートである。

図 3 3 は図 2 7 のスカラー倍計算部におけるスカラー倍計算方法を示すフローチャートである。

図 3 4 は本発明の第 1 4 実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

- 25 図 3 5 は本発明の第 1 5 実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図 3 6 は本発明の第 1 6 実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図 3 7 は本発明の第 1 7 実施例のスカラー倍計算方法における座標復元方法を

示すフローチャート図である。

図38は本発明の第18実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図39は本発明の第19実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図40は本発明の第20実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図41は本発明の第21実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図42は本発明の第22実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図43は本発明の第16実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図44は本発明の第17、第18及び第19実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図45は本発明の第22実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面により説明する。

図1は暗号/復号処理装置の構成を示したものである。この暗号/復号処理装置101は、入力されたメッセージの暗号化、暗号化されたメッセージの復号化のいずれも行えるようにしたものである。尚、ここで扱う楕円曲線は標数5以上の楕円曲線とする。

入力されたメッセージを暗号化し、暗号化されたメッセージを復号化する場合、一般に次の数1が成立する。

$$P_m + k(aQ) - a(kQ) = P_m \quad \dots \text{数1}$$

ここで、 P_m はメッセージであり、 k は乱数、 a は秘密鍵を示す定数、 Q は定点である。この式の $P_m + k(aQ)$ の aQ は、公開鍵を示しており、入力されたメッセージを公開鍵によって暗号化することを示している。 $a(kQ)$ の a は

秘密鍵を示しており、秘密鍵により復号化することを示している。

従って、図1に示した暗号/復号処理装置101をメッセージの暗号化だけに用いる場合には、 $P_m + k(aQ)$ 及び kQ を計算して出力し、復号化だけに用いる場合には、秘密鍵 a 及び kQ より $-a(kQ)$ を計算し、 $(P_m + k(aQ)) - a(kQ)$ を計算して出力するようにすればよい。

図1に示した暗号/復号処理装置101は、処理部110と、記憶部120、レジスタ部130とを有している。処理部120は、暗号化処理に必要な処理を機能ブロックで示しており、入力されたメッセージの暗号化や暗号化されたメッセージの復号化を行う暗号/復号処理部102、暗号/復号処理部102で暗号化
10 や復号化を行うのに必要なパラメータを演算するスカラー倍計算部103とを有している。記憶部120は、定数、秘密情報（例えば、秘密鍵である。）などを記憶している。レジスタ部130は、暗号化又は復号化処理において演算の結果や、記憶部120に記憶された情報を一次的に記憶する。尚、処理部110、レジスタ部130は以下に説明する処理を行う専用の演算装置やCPUなどにより
15 実現することができ、記憶部120は、RAM、ROMなどによって実現することができる。

次に、図1に示した暗号/復号処理装置101の動作について説明する。図3は、暗号/復号処理装置101において暗号化、復号化を行う場合の各部の情報の伝達を示したものである。

20 暗号/復号処理部102は暗号化処理を行なう場合は暗号化処理部102と表記し、復号化処理を行なう場合は復号化処理部102と表記する。

まず、図30により入力されたメッセージを暗号化する場合の動作について説明する。

暗号/復号処理部102へメッセージが入力されると(3001)、入力された
25 たメッセージのビット長が予め定めたビット長か否かを判断する。予め定めたビット長より長い場合には、予め定めたビット長となるようにメッセージを区切る（以下、メッセージは所定のビット長に区切られているものとして説明する。）。次に、暗号/復号処理部102は、メッセージのビット列によって表される数値を x 座標 ($x1$) にもつ楕円曲線上の y 座標の値 ($y1$) を計算する。例えば、モ

モンゴメリ型楕円曲線は、 $By^2 = x^3 + Ax^2 + x$ で表されるので、これより y 座標の値を求めることができる。尚、 B 、 A はそれぞれ定数である。暗号化処理部 102 は、公開鍵 aQ 及び Q の x 座標、 y 座標の値をスカラー倍計算部 103 へ送る。このとき、暗号化処理部 102 は乱数を生成し、これをスカラー倍計算部 103 へ送る (3002)。スカラー倍計算部 103 は、 Q の x 座標、 y 座標の値、乱数によるスカラー倍点 (x_{d1} 、 y_{d1}) と、公開鍵 aQ の x 座標、 y 座標の値、乱数によるスカラー倍点 (x_{d2} 、 y_{d2}) とを計算し (3003)、計算されたスカラー倍点を暗号化処理部 102 へ送る (3004)。暗号化処理部 102 は、送られたスカラー倍点を用いて、暗号化処理を行う (3005)。例えば、モンゴメリ型の楕円曲線については、次式により暗号化されたメッセージ x_{e1} 、 x_{e2} を得る。

$$x_{e1} = B \left((y_{d1} - y_1) / (x_{d1} - x_1) \right)^2 - A - x_1 - x_{d1} \quad \cdots \text{数 2}$$

$$x_{e2} = x_{d2} \quad \cdots \text{数 3}$$

暗号/復号処理装置 101 は暗号/復号処理部 102 で暗号化されたメッセージ 15 を出力する。

次に、図 32 により暗号化されたメッセージを復号化する場合の動作について説明する。

暗号/復号処理部 102 へ暗号化されたメッセージが入力されると (3201)、暗号化されたメッセージのビット列によって表される数値を x 座標にもつ楕円曲線上の y 座標の値を計算する。ここで、暗号化されたメッセージが x_{e1} 、 x_{e2} のビット列であり、モンゴメリ型楕円曲線の場合、 y 座標の値 (y_{e1}) は $By_{e1}^2 = x_{e1}^3 + Ax_{e1}^2 + x_{e1}$ から得られる。尚、 B 、 A はそれぞれ定数である。暗号/復号処理部 102 は、 x 座標、 y 座標の値 (x_{e1} 、 y_{e1}) をスカラー倍計算部 103 へ送る (3202)。スカラー倍計算部 103 は記憶部 120 から秘密情報を読み出し (3203)、 x 座標、 y 座標の値、秘密情報からスカラー倍点 (x_{d3} 、 y_{d3}) を計算し (3204)、計算されたスカラー倍点を暗号/復号処理部 102 へ送る (3205)。暗号/復号処理部 102 は、送られたスカラー倍点を用いて、復号化処理を行う (3206)。例えば、暗号化されたメッセージが、 x_{e1} 、 x_{e2} のビット列であり、モンゴメリ型の楕円曲線の場合は、

次式により x_{f1} を得る。

$$x_{f1} = B((y_{e2} + y_{d3}) / (x_{e2} - x_{d3}))^2 - A - x_{e2} - x_{d3} \quad \cdots \text{数 4}$$

この x_{f1} は、暗号化される前のメッセージ x_1 に相当するものである。

復号処理部 102 は復号化されたメッセージ x_{f1} を出力する (3207)

- 5 以上のようにして、暗号/復号処理部 102 により暗号化、または復号化処理が行われる。

次に、暗号化処理装置 101 のスカラー倍計算部 103 の処理について説明する。ここでは、暗号化処理装置 101 が、復号化処理を行う場合を例に以下、説明する。

- 10 図 2 は、スカラー倍計算部 103 の機能ブロックを示したものである。図 25 は、スカラー倍計算部 103 の動作を示したものである。

- 高速スカラー倍計算部 202 が、秘密情報であるスカラー値及び暗号化されたメッセージと、暗号化されたメッセージが X 座標となる楕円曲線上の Y 座標の値である楕円曲線上の点を受け取る (ステップ 2501) と、高速スカラー倍計算部 202 は受け取ったスカラー値と楕円曲線上の点からスカラー倍点の座標の一部の値を計算し (ステップ 2502)、その情報を座標復元部 203 に与える (ステップ 2503)。座標復元部 203 は与えられたスカラー倍点の情報及び入力された楕円曲線上の点よりスカラー倍点の座標の復元を行なう (ステップ 2504)。スカラー倍計算部 103 は完全に座標が与えられたスカラー倍点を計算結果として出力する (ステップ 2505)。ここで、完全に座標が与えられたスカラー倍点とは、y 座標が計算されて出力されることを意味する (以下、同じ。)
- 15 202 は受け取ったスカラー値と楕円曲線上の点からスカラー倍点の座標の一部の値を計算し (ステップ 2502)、その情報を座標復元部 203 に与える (ステップ 2503)。座標復元部 203 は与えられたスカラー倍点の情報及び入力された楕円曲線上の点よりスカラー倍点の座標の復元を行なう (ステップ 2504)。スカラー倍計算部 103 は完全に座標が与えられたスカラー倍点を計算結果として出力する (ステップ 2505)。ここで、完全に座標が与えられたスカラー倍点とは、y 座標が計算されて出力されることを意味する (以下、同じ。)
- 20 以下、スカラー倍計算部 103 の高速スカラー倍計算部 202、座標復元部 203 についていくつかの実施例を説明する。

- 第 1 の実施例は、スカラー倍計算部 103 がスカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものである。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P から
- 25 円曲線上の点 P から、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものである。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P から

- モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部203に与える。座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部103はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。
- 10 次に図11により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に x_d, y_d を出力する座標復元部の処理について説明する。
- 座標復元部203では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線における
- 15 スカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。
- 20 ステップ1101において $X_d \times x$ が計算され、レジスタ T_1 に格納される。ステップ1102において $T_1 - Z_d$ が計算される。ここでレジスタ T_1 には $X_d x$ が格納されており、したがって $X_d x - Z_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ1103において $Z_d \times x$ が計算され、レジスタ T_2 に格納される。ステップ1104において $X_d - T_2$ が計算される。ここでレジスタ T_2

- には $Z_d x$ が格納されており、したがって $X_d - xZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1105において $X_{d+1} \times T_2$ が計算される。ここでレジスタ T_2 には $X_d - xZ_d$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ1106において
- 5 T_2 の2乗が計算される。ここでレジスタ T_2 には $(X_d - xZ_d)$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1107において $T_2 \times X_{d+1}$ が計算される。ここでレジスタ T_2 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1108において $T_2 \times Z_{d+1}$
- 10 が計算される。ここでレジスタ T_2 には $X_{d+1} (X_d - xZ_d)^2$ が格納されており、したがって $Z_{d+1} X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1109において $T_2 \times y$ が計算される。ここでレジスタ T_2 には $Z_{d+1} X_{d+1} (X_d - xZ_d)^2$ が格納されており、したがって $yZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1
- 15 110において $T_2 \times B$ が計算される。ここでレジスタ T_2 には $yZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が格納されており、したがって $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1111において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が格納されており、したがって $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が計算される。その結果が
- 20 レジスタ T_2 に格納される。ステップ1112において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が格納されており、したがって $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d X_d$ が計算される。その結果がレジスタ T_4 に格納される。ステップ1113において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が格納されており、したがって
- 25 $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1114においてレジスタ T_2 の逆元が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d^2$ が格納されており、したがって $1/ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1115において $T_2 \times T_4$ が計算される。ここでレジスタ

- T_2 には $1/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$ がレジスタ T_4 には $ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d$ がそれぞれ格納されており、したがって $(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d)/(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2)(=X_d/Z_d)$ が計算される。その結果がレジスタ x_d に格納される。ステップ1116において $T_1 \times Z_{d+1}$ が計算される。ここでレジスタ T_1 には X_dx-Z_d が格納されており、したがって $Z_{d+1}(X_dx-Z_d)$ が計算される。その結果がレジスタ T_4 に格納される。ステップ1117においてレジスタ T_1 の2乗が計算される。ここでレジスタ T_1 には (X_dx-Z_d) が格納されており、したがって $(X_dx-Z_d)^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ1118において $T_1 \times T_2$ が計算される。
- 10 ここでレジスタ T_1 には $(X_dx-Z_d)^2$ がレジスタ T_2 には $1/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2$ がそれぞれ格納されており、したがって $(X_dx-Z_d)^2/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1119において T_3+T_4 が計算される。ここでレジスタ T_3 には $X_{d+1}(X_d-xZ_d)$ がレジスタ T_4 には $Z_{d+1}(X_dx-Z_d)$ がそれぞれ格納されており、したがって $X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ1120において T_3-T_4 が計算される。ここでレジスタ T_3 には $X_{d+1}(X_d-xZ_d)$ がレジスタ T_4 には $Z_{d+1}(X_dx-Z_d)$ がそれぞれ格納されており、したがって $X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ1121において $T_1 \times T_3$ が計算される。ここでレジスタ T_1 には $X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)$ がレジスタ T_3 には $X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)$ がそれぞれ格納されており、したがって $\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)\}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ1122において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)\}$ がレジスタ T_2 には $(X_dx-Z_d)^2/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$ がそれぞれ格納されており、したがって
- $$\frac{\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)\}(X_dx-Z_d)^2}{ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2}$$

が計算される。その結果が y_d に格納される。 x_d にはステップ 1 1 1 5 において $(ByZ_{d+1}X_{d+1}(X_d - xZ_d)^2 Z_d X_d) / (ByZ_{d+1}X_{d+1}(X_d - xZ_d)^2 X_d^2)$ が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により座標復元部 2 0 3 へ与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、

- 5 Z_{d+1} からモンゴメリ型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における値が全て復元される理由は以下の通りである。尚、点 $(d+1)P$ は点 dP に点 P を加算した点であり、点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、次の式を得る。

$$(A + x + x_d + x_{d+1})(x_d - x)^2 = B(y_d - y)^2 \quad \cdots \text{数 6}$$

$$10 \quad (A + x + x_d + x_{d+1})(x_d - x)^2 = B(y_d + y)^2 \quad \cdots \text{数 7}$$

両辺を各々減算することにより、

$$(x_{d-1} - x_{d+1})(x_d - x)^2 = 4By_d y \quad \cdots \text{数 8}$$

を得る。したがって、

$$y_d = (x_{d-1} - x_{d+1})(x_d - x)^2 / 4By \quad \cdots \text{数 9}$$

- 15 となる。ここで $x_d = X_d / Z_d$ 、 $x_{d+1} = X_{d+1} / Z_{d+1}$ 、 $x_{d-1} = X_{d-1} / Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2 / 4ByZ_{d-1}Z_{d+1}Z_d^2 \quad \cdots \text{数 10}$$

モンゴメリ型楕円曲線の射影座標での加算公式は

$$20 \quad X_{m+n} = Z_{m-n} [(X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)]^2 \quad \cdots \text{数 11}$$

$$Z_{m+n} = X_{m-n} [(X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)]^2 \quad \cdots \text{数 12}$$

である。ここで X_m 及び Z_m はモンゴメリ型楕円曲線上の点 P の m 倍点 mP の射影座標における X 座標及び Z 座標、 X_n 及び Z_n はモンゴメリ型楕円曲線上の点 P の n 倍

- 25 点 nP の射影座標における X 座標及び Z 座標、 X_{m-n} 及び Z_{m-n} はモンゴメリ型楕円曲線上の点 P の $(m-n)$ 倍点 $(m-n)P$ の射影座標における X 座標及び Z 座標、 X_{m+n} 及び Z_{m+n} はモンゴメリ型楕円曲線上の点 P の $(m+n)$ 倍点 $(m+n)P$ の射影座標における X 座標及び Z 座標であり、 m 、 n は $m > n$ をみたす正整数である。この式は $X_m / Z_m = x_m$ 、 $X_n / Z_n = x_n$ 、 $X_{m-n} / Z_{m-n} = x_{m-n}$ が不変のとき、 X_{m+n} / Z_{m+n}

$= x_{m+n}$ も不変となるので、射影座標での公式としてうまく働いている。他方、

$$X'_{m-n} = Z_{m+n} [(X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)]^2 \quad \cdots \text{数 } 1 \ 3$$

$$Z'_{m-n} = X_{m+n} [(X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)]^2 \quad \cdots \text{数 } 1 \ 4$$

とおくと、この式で $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m+n}/Z_{m+n} = x_{m+n}$ が不

- 5 変のとき、 X'_{m-n}/Z'_{m-n} も不変となる。また、 $X'_{m-n}/Z'_{m-n} = X_{m-n}/Z_{m-n}$ をみたすので、 x_{m-n} の射影座標として X'_{m-n}, Z'_{m-n} をとってよい。

$m=d, n=1$ として上記公式を用いて y_d の式より X_{d-1} 及び Z_{d-1} を消去し、

$X_1 = x, Z_1 = 1$ とおくことにより、次の式を得る。

$$y_d = \frac{\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - x Z_d)\} \{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - x Z_d)\} (X_d x - Z_d)^2}{ByZ_{d+1}X_{d+1}(X_d - x Z_d)^2 Z_d^2}$$

10

$\cdots \text{数 } 1 \ 5$

$x_d = X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d の分母と通分することにより、

$$x_d = \frac{ByZ_{d+1}X_{d+1}Z_d(X_d - x Z_d)^2 X_d}{ByZ_{d+1}X_{d+1}Z_d(X_d - x Z_d)^2 Z_d} \quad \cdots \text{数 } 1 \ 6$$

- 15 となる。ここで、 x_d, y_d は図 1 1 の処理により与えられている。したがって、アフィン座標 (x_d, y_d) の値が全て復元されていることになる。

- 上記手順はステップ 1 1 0 1、ステップ 1 1 0 3、ステップ 1 1 0 5、ステップ 1 1 0 7、ステップ 1 1 0 8、ステップ 1 1 0 9、ステップ 1 1 1 0、ステップ 1 1 1 1、ステップ 1 1 1 2、ステップ 1 1 1 3、ステップ 1 1 1 5、ステップ 20 プ 1 1 1 6、ステップ 1 1 1 8、ステップ 1 1 2 1 及びステップ 1 1 2 2 において有限体上の乗算の計算量を必要とする。また、ステップ 1 1 0 6 及びステップ 1 1 1 7 において有限体上の 2 乗算の計算量を必要とする。また、ステップ 1 1 1 4 において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S 及び有限体上の逆元演算の計算量を I とすると、上記 25 手順は $15M + 2S + I$ の計算量を必要とする。これは高速スカラー倍計算の計

算量と比べてはるかに小さい。例えばスカラー値 d が160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500M弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は56.6Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元でき

5 ていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた x_d, y_d の値が計算できれば x_d, y_d の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメータである B の値を小さくすることにより、ステップ1110における乗算の計算量を削減することがで

10 きる。

次に図4により、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力する高速スカラー倍計算部の処理を説明する。

高速スカラー倍計算部202では、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点 P を入力し、以下の手順によりモンゴメリ型楕円曲線に

15 おいて射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ のうち X_{d+1} 及び Z_{d+1} を出力する。ステップ401として、変数 I に初期値1を代入する。ステップ402として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標にお

20 ける2倍算の公式を用いて2倍点 $2P$ を計算する。ステップ403として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ402で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ404として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すればステップ413へ行く。一致しなければステップ40

25 5へ行く。ステップ405として、変数 I を1増加させる。ステップ406として、スカラー値の I 番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ407へ行く。そのビットの値が1であればステップ410へ行く。ステップ407として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算す

- る。その後ステップ408へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ408として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ409へ行く。ここで、2倍算 $2(mP)$ は、モン
- 5 ギョメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ409として、ステップ408で求めた点 $2mP$ とステップ407で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ404へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ410として、射影
- 10 座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ411へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ411として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステッ
- 15 プ412へ行く。ここで、2倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ412として、ステップ410で求めた点 $(2m+1)P$ とステップ411で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ404へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、点 mP 及び点 $(m+1)P$ は全て射
- 20 影座標において表されている。ステップ413として、射影座標で表された点の組 $(mP, (m+1)P)$ から、射影座標で表された点 $mP=(X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d として、射影座標で表された点 $(m+1)P=(X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} として、出力する。ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及
- 25 び2倍算の公式では Y 座標を求める事ができないので、求まっていない。また上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ とすることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限

- 体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M + 2S$ である。スカラー値のI番目のビットの値が0であれば、ステップ407において加算の計算量、ステップ408において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要となる。スカラー値
- 5 のI番目のビットの値が1であれば、ステップ410において加算の計算量、ステップ411において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要である。いずれの場合においても $6M + 4S$ の計算量が必要である。ステップ404、ステップ405、ステップ406、ステップ407、ステップ408、ステップ409乃至はステップ404、ステップ405、ステップ406、
- 10 ステップ410、ステップ411、ステップ412の繰り返しの回数は、(スカラー値dのビット長) - 1回となるので、ステップ402での2倍算の計算量を考慮に入れると、全体の計算量は $(6M + 4S)(k - 1) + 3M + 2S$ となる。ここでkはスカラー値dのビット長である。一般的には、計算量Sは、 $S = 0.8M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k - 4.6)M$
- 15 となる。例えばスカラー値dが160ビット($k = 160$)であれば、上記手順のアルゴリズムの計算量はおおよそ1467Mとなる。スカラー値dのビットあたりの計算量としてはおおよそ9.2Mとなる。A.Miyaji, T.Ono, H.Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998)
- 20 pp.51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ10Mと見積もられる。例えばスカラー値dが160ビット($k = 160$)であれば、このスカラー倍計算方法の計算量はおお
- 25 よそ1600Mとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部202において上記手順のアルゴリズムを用いなくとも、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、 $X_d, Y_d, X_{d+1}, Z_{d+1}$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用

いていもよい。

- スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $15M + 2S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k - 4.6)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M$ 、 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 52)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量は 1524M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおよそ 1640M であり、これと比べて必要となる計算量は削減されている。

- 第 2 の実施例は、スカラー倍計算部 103 がスカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、モンゴメリ型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算し出力するものである。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 x 及び y よりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標 X_d 、 Y_d 及び Z_d の復元を行なう。スカラー倍計算部 103 は射影座標において完全に座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算結果として出力する。

次に図 9 により、座標 x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} が与えられた場合に X_d 、

Y_d 、 Z_d を出力する座標復元部の処理について説明する。

- 座標復元部 203では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部 103に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した (x, y) を入力し、以下の手順で射影座標において完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるス
- 10 カラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。
- 15 ステップ901において $X_d \times x$ が計算され、レジスタ T_1 に格納される。ステップ902において $T_1 - Z_d$ が計算される。ここでレジスタ T_1 には $X_d x$ が格納されており、したがって $X_d x - Z_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ903において $Z_d \times x$ が計算され、レジスタ T_2 に格納される。ステップ904において $X_d - T_2$ が計算される。ここでレジスタ T_2 には $Z_d x$ が
- 20 格納されており、したがって $X_d - xZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ905において $Z_{d+1} \times T_1$ が計算される。ここでレジスタ T_1 には $X_d x - Z_d$ が格納されており、したがって $Z_{d+1} (X_d x - Z_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ906において $X_{d+1} \times T_2$ が計算される。ここでレジスタ T_2 には $X_d - xZ_d$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)$ が計算される。その結果がレジスタ T_4 に格納される。ス
- 25 テップ907において T_1 の2乗が計算される。ここでレジスタ T_1 には $X_d x - Z_d$ が格納されており、したがって $(X_d x - Z_d)^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ908において T_2 の2乗が計算される。ここでレジスタ T_2 には $X_d - xZ_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算

- される。その結果がレジスタ T_2 に格納される。ステップ 909 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $(X_d - xZ_d)^2$ が格納されており、したがって $Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。
- ステップ 910 において $T_2 \times X_{d+1}$ が計算される。ここでレジスタ T_2 には
- 5 $Z_d (X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 911 において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 に $X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 912 において $T_2 \times y$ が計算される。ここでレ
- 10 ジスタ T_2 には $Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $y Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 913 において $T_2 \times B$ が計算される。ここでレジスタ T_2 には $y Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $By Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 9
- 15 14 において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $By Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $By Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 X_d$ が計算される。その結果が X_d に格納される。ステップ 915 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $By Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $By Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d$ が計算される。その結果
- 20 がレジスタ Z_d に格納される。ステップ 916 において $T_3 + T_4$ が計算される。ここでレジスタ T_3 には $Z_{d+1} (X_d x - Z_d)$ がレジスタ T_4 には $X_{d+1} (X_d - xZ_d)$ が格納されており、したがって $Z_{d+1} (X_d x - Z_d) + X_{d+1} (X_d - xZ_d)$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 917 において $T_3 - T_4$ が計算される。ここでレジスタ T_3 には $Z_{d+1} (X_d x - Z_d)$ がレジスタ T_4 には
- 25 $X_{d+1} (X_d - xZ_d)$ が格納されており、したがって $Z_{d+1} (X_d x - Z_d) - X_{d+1} (X_d - xZ_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 918 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(X_d x - Z_d)^2$ がレジスタ T_2 には $Z_{d+1} (X_d x - Z_d) + X_{d+1} (X_d - xZ_d)$ が格納されており、したがって $\{Z_{d+1} (X_d x - Z_d) + X_{d+1} (X_d - xZ_d)\} (X_d x - Z_d)^2$ が計算される。その結

- 果がレジスタ T_1 に格納される。ステップ 9 1 9 において $T_1 \times T_3$ が計算される。ここでレジスタ T_1 には $\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$ がレジスタ T_3 には $Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)$ が格納されており、したがって $\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}\{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$ が計算される。その結果がレジスタ Y_d に格納される。したがってレジスタ Y_d には $\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}\{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$ が格納されている。レジスタ X_d にはステップ 9 1 4 において $By Z_{d+1} X_{d+1} Z_{d+1}(X_d - xZ_d)^2 X_d$ が格納され、その後更新が行われないので、その値が保持されている。レジスタ Z_d にはステップ 9 1 5 において $By Z_{d+1} X_{d+1} Z_{d+1}(X_d - xZ_d)^2 Z_d$ が格納され、その後更新が行われないので、その値が保持されている。

- 上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} からスカラー倍点の射影座標 (X_d, Y_d, Z_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点であり、点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、次の数 6、数 7 を得る。両辺を各々減算することにより、数 8 を得る。したがって、数 9 となる。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ 、 $x_{d-1} = X_{d-1}/Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、数 10 を得る。

- 20 モンゴメリ型楕円曲線の射影座標での加算公式は数 11、数 12 である。ここで X_m 及び Z_m はモンゴメリ型楕円曲線上の点 P の m 倍点 mP の射影座標における X 座標及び Z 座標、 X_n 及び Z_n はモンゴメリ型楕円曲線上の点 P の n 倍点 nP の射影座標における X 座標及び Z 座標、 X_{m-n} 及び Z_{m-n} はモンゴメリ型楕円曲線上の点 P の $(m-n)$ 倍点 $(m-n)P$ の射影座標における X 座標及び Z 座標、 X_{m+n} 及び Z_{m+n} はモンゴメリ型楕円曲線上の点 P の $(m+n)$ 倍点 $(m+n)P$ の射影座標における X 座標及び Z 座標であり、 m 、 n は $m > n$ をみたす正整数である。この式は $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m-n}/Z_{m-n} = x_{m-n}$ が不変のとき、 $X_{m+n}/Z_{m+n} = x_{m+n}$ も不変となるので、射影座標での公式としてうまく働いている。他方、数 14、数 15 とおくと、この式で $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m+n}/Z_{m+n} = x_{m+n}$ が

不変のとき、 X'_{m-n}/Z'_{m-n} も不変となる。また、 $X'_{m-n}/Z'_{m-n}=X_{m-n}/Z_{m-n}=x_{m-n}$ をみたすので、 x_{m-n} の射影座標として X'_{m-n}, Z'_{m-n} をとつてよい。 $m=d, n=1$ として上記公式を用いて y_d の式より X_{d-1} 及び Z_{d-1} を消去し、 $X_1=x, Z_1=1$ とおくことにより、数15を得る。 $x_d=X_d/Z_d$ であるが、

5 y_d の分母と通分することにより、数16となる。

その結果として、

$$Y_d = \{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - x Z_d)\} \{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - x Z_d)\} (X_d x - Z_d)^2$$

…数17

10 とし、 X_d 及び Z_d をそれぞれ

$$ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 X_d \quad \cdots \text{数18}$$

$$ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 Z_d \quad \cdots \text{数19}$$

により更新すればよい。ここで、 X_d, Y_d, Z_d は図9の処理により与えられている。したがって、射影座標 (X_d, Y_d, Z_d) の値が全て復元されていることになる。

15 上記手順はステップ901、ステップ903、ステップ905、ステップ906、ステップ909、ステップ910、ステップ911、ステップ912、ステップ913、ステップ914、ステップ915、ステップ918及びステップ919において有限体上の乗算の計算量を必要とする。また、ステップ907及びステップ908において有限体上の2乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の2乗算の計算量をSとすると、上記手順は $13M + 2S$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500M弱と見

25 積もられる。 $S = 0.8M$ と仮定すると座標復元の計算量は $14.6M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた X_d, Y_d, Z_d の値が計算できれば X_d, Y_d, Z_d の値が復元できる。また、 x_d, y_d が上記計算式に

より与えられる値を取るように X_d 、 Y_d 、 Z_d の値を選択し、その値が計算できれば X_d 、 Y_d 、 Z_d が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタである B の値を小さくとることにより、ステップ913における乗算の計算量を削減することができる。

- 5 次に、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムについて説明する。

第2実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、第1実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部202において上記アルゴリズムを用いなくても、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部103における座標復元部203の座標復元に必要な計算量は13M+2Sであり、これは高速スカラー倍計算部202の高速スカラー倍計算に必要な計算量の $(9.2k-4.6)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S=0.8M$ と仮定すると、この計算量はおよそ $(9.2k+10)M$ と見積もることができる。例えばスカラー値 d が160ビット($k=160$)であれば、このスカラー倍計算に必要な計算量は1482Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要な計算量はおよそ1600Mであり、これと比べて必要となる計算量は削減されている。

第3の実施例は、スカラー倍計算部103がスカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものである。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部103に入力す

- ると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}, x$ 及び y よりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部 103 はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。

- 次に図 12 により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ が与えられた場合に x_d, y_d を出力する座標復元部の処理について説明する。

- 座標復元部 203 では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} 、スカラー倍計算部 103 に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- ステップ1201において $X_{d-1} \times Z_{d+1}$ が計算され、レジスタ T_1 に格納される。ステップ1202において $Z_{d-1} \times X_{d+1}$ が計算され、レジスタ T_2 に格納される。ステップ1203において $T_1 - T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1} Z_{d+1}$ がレジスタ T_2 には $Z_{d-1} X_{d+1}$ がそれぞれ格納されており、したがって $X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1}$ が計算される。その結果がレジスタ
- 5 T_1 に格納される。ステップ1204において $Z_d \times x$ が計算され、レジスタ T_2 に格納される。ステップ1205において $X_d - T_2$ が計算される。ここでレジスタ T_2 には $Z_d x$ が格納されており、したがって $X_d - x Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1206において T_2 の2乗が計算される。
- 10 ここでレジスタ T_2 には $X_d - x Z_d$ が格納されており、したがって $(X_d - x Z_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1207において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1}$ がレジスタ T_2 には $(X_d - x Z_d)^2$ がそれぞれ格納されており、したがって $(X_d - x Z_d)^2 (X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1})$ が計算される。その結果がレジスタ T_1 に格
- 15 納される。ステップ1208において $4B \times y$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1209において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $4By$ が格納されており、したがって $4By Z_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1210において $T_2 \times Z_{d-1}$ が計算される。ここでレジスタ T_2 には $4By Z_{d+1}$ が格納されており、し
- 20 たがって $4By Z_{d-1} Z_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1211において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4By Z_{d+1} Z_{d-1}$ が格納されており、したがって $4By Z_{d+1} Z_{d-1} Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1212において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $4By Z_{d-1} Z_{d+1} Z_d$ が格納されており、し
- 25 たがって $4By Z_{d+1} Z_{d-1} Z_d X_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ1213において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4By Z_{d+1} Z_{d-1} Z_d$ が格納されており、したがって $4By Z_{d+1} Z_{d-1} Z_d Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1214においてレジスタ T_2 の逆元が計算される。ここでレジスタ T_2 には $4By Z_{d+1} Z_{d-1} Z_d Z_d$ が

- 格納されており、したがって $1/4ByZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1 2 1 5 において $T_2 \times T_3$ が計算される。ここでレジスタ T_2 には $1/4ByZ_{d+1}Z_{d-1}Z_dZ_d$ がレジスタ T_3 には $4ByZ_{d+1}Z_{d-1}Z_dX_d$ がそれぞれ格納されており、したがって $(4ByZ_{d+1}Z_{d-1}Z_dX_d)/(4ByZ_{d+1}Z_{d-1}Z_dZ_d)$ が計算される。その結果がレジスタ x_d に格納される。ステップ 1 2 1 6 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(X_d - x_d)^2 (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ がレジスタ T_2 には $1/4ByZ_{d+1}Z_{d-1}Z_dZ_d$ がそれぞれ格納されており、したがって $(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - x_d)^2 / 4ByZ_{d-1}Z_{d+1}Z_d^2$ が計算される。その結果がレジスタ y_d に格納される。したがってレジスタ y_d には $(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - x_d)^2 / 4ByZ_{d-1}Z_{d+1}Z_d^2$ が格納されている。レジスタ x_d にはステップ 1 2 1 5 において $(4ByZ_{d+1}Z_{d-1}Z_dX_d)/(4ByZ_{d+1}Z_{d-1}Z_dZ_d)$ が格納され、その後更新が行なわれないので、その値が保持されている。

- 上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 X_{d-1} 、 Z_{d-1} からモンゴメリ型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点であり、点 $(d-1)P$ は点 dP から点 P を減算した点である。

- モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 6、数 7 を得る。両辺を各々減算することにより、数 8 を得る。したがって、数 9 となる。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ 、 $x_{d-1} = X_{d-1}/Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、数 10 を得る。

$x_d = X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d の分母と通分することにより、

$$x_d = \frac{4ByZ_{d+1}Z_{d-1}Z_dX_d}{4ByZ_{d+1}Z_{d-1}Z_dZ_d} \quad \dots \text{数 } 20$$

となる。この x_d 、 y_d は図 1 2 で示した処理により与えられ、したがってアフィン座標 (x_d, y_d) の値が全て復元されていることになる。

上記手順はステップ 1 2 0 1、ステップ 1 2 0 2、ステップ 1 2 0 4、ステッ

- プ1207、ステップ1208、ステップ1209、ステップ1210、ステップ1211、ステップ1212、ステップ1213、ステップ1215及びステップ1216において有限体上の乗算の計算量を必要とする。また、ステップ1206において有限体上の2乗算の計算量を必要とする。また、ステップ1214において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の2乗算の計算量をS及び有限体上の逆元演算の計算量をIとすると、上記手順は $12M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500M弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は52.8Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。
- 15 尚、上記手順をとらなくても、上記計算式により与えられた x_d, y_d の値が計算できれば x_d, y_d の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBの値を小さくすることにより、ステップ1208における乗算の計算量を削減することができる。
- 20 次に図5により、スカラー値d及びモンゴメリ型楕円曲線上の点Pから $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力する高速スカラー倍計算部の処理について説明する。
- 高速スカラー倍計算部202では、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ のうち X_{d-1} 及び Z_{d-1} を出力する。ステップ501として、変数Iに初期値1を代入する。ステップ502として、点Pの2

- 倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて 2 倍点 $2P$ を計算する。
- ステップ 503 として、スカラー倍計算部 103 に入力された楕円曲線上の点 P とステップ 502 で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ 504 として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すれば $m=d$ となり、ステップ 514 へ行く。一致しなければステップ 505 へ行く。ステップ 505 として、変数 I を 1 増加させる。ステップ 506 として、スカラー値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 507 へ行く。そのビットの値が 1 であればステップ 510 へ行く。ステップ 507 として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 508 へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ 508 として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の 2 倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ 509 へ行く。ここで、2 倍算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算される。ステップ 509 として、ステップ 508 で求めた点 $2mP$ とステップ 507 で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 504 へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ 510 として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 511 へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ 511 として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の 2 倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ 512 へ行く。ここで、2 倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算される。ステップ 512 として、ステップ 510 で求めた点 $(2m+1)P$ とステップ 511 で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組

- (mP , $(m+1)P$)の代わりに格納する。その後ステップ504へ戻る。ここで、点($2m+1$) P 、点($2m+2$) P 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。
- ステップ514として、射影座標で表された点の組(mP , $(m+1)P$)から、点 $(m-1)P$ の射影座標における X 座標 X_{m-1} 及び Z 座標 Z_{m-1} を求め、それぞれ X_{d-1} 及び
- 5 Z_{d-1} とする。その後ステップ513へ行く。ステップ513として、射影座標で表された点 $mP = (X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d として、射影座標で表された点 $(m+1)P = (X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} として、 X_{d-1} 及び Z_{d-1} と共に出力する。ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び2倍算の
- 10 公式では Y 座標を求める事ができないので、求まっていない。また上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ514において $(m-1)P$ を求める際に、数10、数11の公式により求めてもよいし、 m が奇数であれば、 $((m-1)/2)P$ の値をステップ512の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の2倍
- 15 算の公式より、 $(m-1)P$ を求めてもよい。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1 = 1$ ととることにより $3M + 2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M + 2S$ である。スカラー値の I 番目のビットの値が0で
- 20 あれば、ステップ507において加算の計算量、ステップ508において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ510において加算の計算量、ステップ511において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要である。いずれの場合においても $6M + 4S$ の計算量が必要である。ス
- 25 テップ504、ステップ505、ステップ506、ステップ507、ステップ508、ステップ509乃至はステップ504、ステップ505、ステップ506、ステップ510、ステップ511、ステップ512の繰り返しの回数は、(スカラー値 d のビット長) - 1回となるので、ステップ502での2倍算の計算量とステップ514での $(m-1)P$ の計算に必要な計算量を考慮に入れると、全体の計算

- 量は $(6M + 4S)k + M$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S = 0.8M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k + 1)M$ となる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、上記手順のアルゴリズムの計算量はおおよそ 1473M となる。
- 5 なる。スカラー値 d のビットあたりの計算量としてはおおよそ $9.2M$ となる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍
- 10 計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ $10M$ と見積もられる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算方法の計算量はおおよそ $1600M$ となる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。
- 15 尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくても、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。
- スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $12M + S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 1)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M$ 、 $S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 53.8)M$ と
- 25 見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量はおおよそ 1526M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおおよそ 164

0 Mであり、これと比べて必要となる計算量は削減されている。

- 第4の実施例は、スカラー倍計算部103がスカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、モンゴメリ型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算し出力する。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部103に入力すると高速ス
- 5 スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部202は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部203に与える。座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}, x$ 及び y よりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標 X_d, Y_d 及び Z_d の復元を行なう。スカラー倍計算部103は射影座標において完全に座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算結果として出力する。
- 10
- 15

次に図13により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ が与えられた場合に X_d, Y_d, Z_d を出力する座標復元部の処理について説明する。

- 20 座標復元部203では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} 、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順で射影座標において完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d)
- 25

で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- 5 ステップ1301において $X_{d-1} \times Z_{d+1}$ が計算され、レジスタ T_1 に格納される。ステップ1302において $Z_{d-1} \times X_{d+1}$ が計算され、レジスタ T_2 に格納される。ステップ1303において $T_1 - T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1} Z_{d+1}$ がレジスタ T_2 には $Z_{d-1} X_{d+1}$ がそれぞれ格納されており、したがって $X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1}$ が計算される。その結果がレジスタ
- 10 T_1 に格納される。ステップ1304において $Z_d \times x$ が計算され、レジスタ T_2 に格納される。ステップ1305において $X_d - T_2$ が計算される。ここでレジスタ T_2 には $Z_d x$ が格納されており、したがって $X_d - x Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1306において T_2 の2乗が計算される。ここでレジスタ T_2 には $X_d - x Z_d$ が格納されており、したがって $(X_d - x Z_d)^2$ が計
- 15 算される。その結果がレジスタ T_2 に格納される。ステップ1307において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1}$ がレジスタ T_2 には $(X_d - x Z_d)^2$ がそれぞれ格納されており、したがって $(X_d - x Z_d)^2 (X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1})$ が計算される。その結果がレジスタ Y_d に格納される。ステップ1308において $4B \times y$ が計算される。その結果がレジスタ
- 20 T_2 に格納される。ステップ1309において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $4By$ が格納されており、したがって $4By Z_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1310において $T_2 \times Z_{d-1}$ が計算される。ここでレジスタ T_2 には $4By Z_{d+1}$ が格納されており、したがって $4By Z_{d+1} Z_{d-1}$ が計算される。その結果がレジスタ T_2 に格納される。ステ
- 25 ップ1311において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4By Z_{d+1} Z_{d-1}$ が格納されており、したがって $4By Z_{d+1} Z_{d-1} Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1312において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $4By Z_{d+1} Z_{d-1} Z_d$ が格納されており、したがって $4By Z_{d+1} Z_{d-1} Z_d X_d$ が計算される。その結果がレジスタ X_d に格納され

る。ステップ1 3 1 3において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4ByZ_{d+1}Z_{d-1}Z_d$ が格納されており、したがって $4ByZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果が Z_d に格納される。したがって Z_d には $4ByZ_{d+1}Z_{d-1}Z_dZ_d$ が格納されている。レジスタ Y_d にはステップ1 3 0 7において $(X_d - xZ_d)^2$

- 5 $(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ が格納され、その後更新が行われないので、その値が保持されている。

上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 X_{d-1} 、 Z_{d-1} からスカラー倍点の射影座標 (X_d, Y_d, Z_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。これより、先に述べた数7を得ることができる。座標復元部2 0 3はスカラー倍点の射影座標で表された完全な座標として (X_d, Y_d, Z_d) を出力する。

上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 X_{d-1} 、 Z_{d-1} からスカラー倍点の射影座標 (X_d, Y_d, Z_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数6、数7を得る。両辺を各々減算することにより、数8を得る。したがって、数9となる。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ 、 $x_{d-1} = X_{d-1}/Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、数7を得る。

$x_d = X_d/Z_d$ であるが、 y_d の分母と通分することにより、数2 0となる。その結果として、

$$Y_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_dx)^2 \quad \cdots \text{数 2 1}$$

とし、 X_d 及び Z_d をそれぞれ

25 $4ByZ_{d+1}Z_{d-1}Z_dX_d \quad \cdots \text{数 2 2}$

$$4ByZ_{d+1}Z_{d-1}Z_dZ_d \quad \cdots \text{数 2 3}$$

により更新すればよい。ここで示した X_d 、 Y_d 、 Z_d は図1 3で示した処理により与えられている。したがって、射影座標の値 (X_d, Y_d, Z_d) が全て復元されることになる。

上記手順はステップ1301、ステップ1302、ステップ1304、ステップ1307、ステップ1308、ステップ1309、ステップ1310、ステップ1311、ステップ1312及びステップ1313において有限体上の乗算の計算量を必要とする。また、ステップ1306において有限体上の2乗算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、2乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の2乗算の計算量をSとすると、上記手順は $10M + S$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500M弱と見積もられる。S=0.8Mと仮定すると座標復元の計算量は10.8Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた X_d, Y_d, Z_d の値が計算できれば X_d, Y_d, Z_d の値が復元できる。また、 x_d, y_d が上記計算式により与えられる値を取るように X_d, Y_d, Z_d の値を選択し、その値が計算できれば X_d, Y_d, Z_d が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメータであるBの値を小さくすることにより、ステップ1308における乗算の計算量を削減することができる。

次に、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムについて説明する。

第4実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、第3実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部202において上記手順のアルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部103における座標復元部203の座標復元に必要な計算量

は $10M + S$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 1)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 11.8)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量はおよそ 1484M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要な計算量はおよそ 1600M であり、これと比べて必要となる計算量は削減されている。

第 5 の実施例は、スカラー倍計算部 103 がスカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力する。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P からモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ の座標のうち x_{d-1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値 x_d 、 x_{d+1} 、 x_{d-1} 、 x 及び y よりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 y_d の復元を行なう。スカラー倍計算部 103 はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。

次に図 26 により、座標 x 、 y 、 x_d 、 x_{d+1} 、 x_{d-1} が与えられた場合に、 x_d 、 y_d を出力する座標復元部の処理について説明する。

- 座標復元部 2 0 3 では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ の座標のうち x_{d-1} 、スカラー倍計算部 1 0 3 に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。

- ステップ 2 6 0 1 において $x_d - x$ が計算され、レジスタ T_1 に格納される。ステップ 2 6 0 2 において T_1 の 2 乗すなわち $(x_d - x)^2$ が計算され、レジスタ T_1 に格納される。ステップ 2 6 0 3 において $x_{d-1} - x_{d+1}$ が計算され、レジスタ T_2 に格納される。ステップ 2 6 0 4 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(x_d - x)^2$ がレジスタ T_2 には $x_{d-1} - x_{d+1}$ がそれぞれ格納されており、したがって $(x_d - x)^2 (x_{d-1} - x_{d+1})$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 2 6 0 5 において $4B \times y$ が計算され、レジスタ T_2 に格納される。ステップ 2 6 0 6 において T_2 の逆元が計算される。ここでレジスタ T_2 には $4By$ が格納されており、したがって $1/4By$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 2 6 0 7 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(x_d - x)^2 (x_{d-1} - x_{d+1})$ がレジスタ T_2 には $1/4By$ がそれぞれ格納されており、したがって $(x_d - x)^2 (x_{d-1} - x_{d+1})/4By$ が計算される。その結果がレジスタ y_d に格納される。したがってレジスタ y_d には $(x_d - x)^2 (x_{d-1} - x_{d+1})/4By$ が格納されている。レジスタ x_d は全く更新されないので入力された値が保持されている。

- 上記手順によりスカラー倍点の y 座標 y_d が復元される理由は以下の通りである。尚、点 $(d+1)P$ は点 dP に点 P を加算した点であり、点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 6、数 7 を得る。

両辺を各々減算することにより、数 8 を得る。したがって、数 9 となる。

ここで、 x_d, y_d は図 2 6 の処理により与えられる。したがって、アフィン座標 (x_d, y_d) の値は全て復元されたことになる。

上記手順はステップ2604、ステップ2605及びステップ2607において有限体上の乗算の計算量を必要とする。また、ステップ2602において有限体上の2乗算の計算量を必要とする。さらにステップ2606において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、2乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の2乗算の計算量を S 、有限体上の逆元演算の計算量を I とすると、上記手順は $3M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500 M 弱と見積もられる。 $S = 0.8M$ 及び $I = 40M$ と仮定すると座標復元の計算量は $43.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば y_d の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタである B の値を小さくすることにより、ステップ2605における乗算の計算量を削減することができる。

次に図6により、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 x_d 、 x_{d+1} 、 x_{d-1} を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部202では、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点 P を入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ のうち x_{d+1} 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ のうち x_{d-1} を出力する。ステップ601として、変数 I に初期値1を代入する。ステップ602として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点 $2P$ を計算する。ステップ603として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ602で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表され

- ている。ステップ604として、変数Iとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ614へ行く。一致しなければステップ605へ行く。ステップ605として、変数Iを1増加させる。ステップ606として、スカラー値のI番目のビットの値が0であるか1であるかを判定する。
- 5 そのビットの値が0であればステップ607へ行く。そのビットの値が1であればステップ610へ行く。ステップ607として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ608へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ608として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ609へ行く。ここで、2倍算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ609として、ステップ608で求めた点 $2mP$ とステップ607で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。
- 15 その後ステップ604へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ610として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ611へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて
- 20 計算される。ステップ611として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ612へ行く。ここで、2倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ612として、ステップ610で求めた点 $(2m+1)P$ とステップ611で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。
- 25 その後ステップ604へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ614として、射影座標で表された点の組 $(mP, (m+1)P)$ から、点 $(m-1)P$ の射影座標におけるX座標 X_{m-1} 及びZ座標 Z_{m-1} を求め、それぞれ X_{d-1} 及び Z_{d-1} とする。その後ステップ615へ行く。

- ステップ6 1 5として、射影座標で表された点 $mP = (X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d とし、射影座標で表された点 $(m+1)P = (X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} とする。ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び2倍算の
- 5 公式では Y 座標を求める事ができないので、求まっていない。 X_{d-1} , Z_{d-1} , X_d , Z_d , X_{d+1} , Z_{d+1} より、

$$x_{d-1} = X_{d-1}Z_dZ_{d+1}/Z_{d-1}Z_dZ_{d+1} \quad \cdots \text{数 } 2 \ 4$$

$$x_d = Z_{d-1}X_dZ_{d+1}/Z_{d-1}Z_dZ_{d+1} \quad \cdots \text{数 } 2 \ 5$$

$$x_{d+1} = Z_{d-1}Z_dX_{d+1}/Z_{d-1}Z_dZ_{d+1} \quad \cdots \text{数 } 2 \ 6$$

- 10 として x_{d-1} , x_d , x_{d+1} を求める。その後ステップ6 1 3へ行く。ステップ6 1 3として、 x_{d-1} , x_d , x_{d+1} を出力する。上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ6 1 4において $(m-1)P$ を求める際に、数1 3、数1 4の公式により求めてもよいし、 m が奇数であれば、 $((m-1)/2)P$ の値をステップ6 1 2の
- 15 段階で別に保持しておき、その値からモンゴメリ型楕円曲線の2倍算の公式より、 $(m-1)P$ を求めてもよい。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ とすることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の
- 20 公式の計算量は、 $3M+2S$ である。スカラー値の I 番目のビットの値が0であれば、ステップ6 0 7において加算の計算量、ステップ6 0 8において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ6 1 0において加算の計算量、ステップ6 1 1において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量
- 25 が必要である。いずれの場合においても $6M+4S$ の計算量が必要である。ステップ6 0 4、ステップ6 0 5、ステップ6 0 6、ステップ6 0 7、ステップ6 0 8、ステップ6 0 9乃至はステップ6 0 4、ステップ6 0 5、ステップ6 0 6、ステップ6 1 0、ステップ6 1 1、ステップ6 1 2の繰り返しの回数は、(スカラー値 d のビット長) - 1回となるので、ステップ6 0 2での2倍算の計算量及

びステップ 6 1 4 での $(m-1)P$ の計算に必要な計算量及びアフィン座標への変換の計算量を考慮に入れると、全体の計算量は $(6M + 4S)k + 11M + I$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S = 0.8M$ 程度、計算量 I は $I = 40M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k + 51)M$ となる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、上記手順のアルゴリズムの計算量はおおよそ 1523M となる。スカラー値 d のビットあたりの計算量としてはおおよそ 9.2M となる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 101514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ 10M と見積もられ、これ以外にアフィン座標への変換の計算量が必要となる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算方法の計算量はおおよそ 1640M となる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 x_d, x_{d+1}, x_{d-1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $3M + S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 51)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ 及び $I = 40M$ と仮定すると、この計算量はおおよそ $(9.2k + 94.8)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量はおおよそ 1567M となる。楕円

曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおよそ1640Mであり、これと比べて必要となる計算量は削減されている。

- 5 第6の実施例は、楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部103の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部103の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部103がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものである。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部103に入力すると高速スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部202は受け取ったス
- 15 カラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1},$
- 20 $Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部203に与える。座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}, x$ 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部103はアフィン座標において完全に座標が与えられ
- 25 たスカラー倍点 (x_d, y_d) を計算結果として出力する。

次に図14により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ が与えられた場合に x_d, y_d を出力する座標復元部の処理について説明する。

座標復元部203では、ワイエルシュトラス型楕円曲線において射影座標で表

- されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} 、スカラー倍計算部 103 に入力されたワイエルシュトラス型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてワイエルシュトラス型楕円曲線
- 10 におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。
- 15 ステップ 1401 において $X_{d-1} \times Z_{d+1}$ が計算され、レジスタ T_1 に格納される。ステップ 1402 において $Z_{d-1} \times X_{d+1}$ が計算され、レジスタ T_2 に格納される。ステップ 1403 において $T_1 - T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1} Z_{d+1}$ がレジスタ T_2 には $Z_{d-1} X_{d+1}$ がそれぞれ格納されており、したがって $X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1}$ が計算される。その結果がレジスタ
- 20 T_1 に格納される。ステップ 1404 において $Z_d \times x$ が計算され、レジスタ T_2 に格納される。ステップ 1405 において $X_d - T_2$ が計算される。ここでレジスタ T_2 には $Z_d x$ が格納されており、したがって $X_d - x Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1406 において T_2 の 2 乗が計算される。ここでレジスタ T_2 には $X_d - x Z_d$ が格納されており、したがって $(X_d - x Z_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1407 において
- 25 $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1}$ がレジスタ T_2 には $(X_d - x Z_d)^2$ がそれぞれ格納されており、したがって $(X_d - x Z_d)^2 (X_{d-1} Z_{d+1} - Z_{d-1} X_{d+1})$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 1408 において $4 \times y$ が計算される。その結果がレ

- ジスタ T_2 に格納される。ステップ 1 4 0 9 において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $4y$ が格納されており、したがって $4yZ_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1 4 1 0 において $T_2 \times Z_{d-1}$ が計算される。ここでレジスタ T_2 には $4yZ_{d+1}$ が格納されており、したがって
- 5 $4yZ_{d+1}Z_{d-1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1 4 1 1 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4yZ_{d+1}Z_{d-1}$ が格納されており、したがって $4yZ_{d+1}Z_{d-1}Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1 4 1 2 において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $4yZ_{d+1}Z_{d-1}Z_d$ が格納されており、したがって
- 10 $4yZ_{d+1}Z_{d-1}Z_dX_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 1 4 1 3 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4yZ_{d-1}Z_{d+1}Z_d$ が格納されており、したがって $4yZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1 4 1 4 においてレジスタ T_2 の逆元が計算される。ここでレジスタ T_2 には $4yZ_{d+1}Z_{d-1}Z_dZ_d$ が格納
- 15 されており、したがって $1/4yZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1 4 1 5 において $T_2 \times T_3$ が計算される。ここでレジスタ T_2 には $1/4yZ_{d+1}Z_{d-1}Z_dZ_d$ がレジスタ T_3 には $4yZ_{d-1}Z_{d+1}Z_dX_d$ がそれぞれ格納されており、したがって $(4yZ_{d+1}Z_{d-1}Z_dX_d) / (4yZ_{d+1}Z_{d-1}Z_dZ_d)$ が計算される。その結果が x_d に格納される。ステップ 1
- 20 4 1 6 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(X_d - xZ_d)^2 (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ がレジスタ T_2 には $1/4yZ_{d+1}Z_{d-1}Z_dZ_d$ がそれぞれ格納されており、したがって $(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1}) (X_d - Z_dx)^2 / 4yZ_{d+1}Z_{d-1}Z_d^2$ が計算される。その結果がレジスタ y_d に格納される。したがってレジスタ y_d には $(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1}) (X_d - Z_dx)^2 / 4yZ_{d-1}Z_{d+1}Z_d^2$ が格納されている。レジスタ x_d にはステップ 1 4 1 5 において $(4yZ_{d-1}Z_{d+1}Z_dX_d) / (4yZ_{d-1}Z_{d+1}Z_dZ_d)$ が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 X_{d-1} 、 Z_{d-1} からワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標

(x_d, y_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、次の式を得る。

$$5 \quad (x + x_d + x_{d+1})(x_d - x)^2 = (y_d - y)^2 \quad \cdots \text{数 } 2 \ 7$$

$$(x + x_d + x_{d-1})(x_d - x)^2 = (y_d + y)^2 \quad \cdots \text{数 } 2 \ 8$$

両辺を各々減算することにより、

$$(x_{d-1} - x_{d+1})(x_d - x)^2 = 4y_d y \quad \cdots \text{数 } 2 \ 9$$

を得る。したがって、

$$10 \quad y_d = (x_{d-1} - x_{d+1})(x_d - x)^2 / 4y \quad \cdots \text{数 } 3 \ 0$$

となる。ここで $x_d = X_d / Z_d$ 、 $x_{d+1} = X_{d+1} / Z_{d+1}$ 、 $x_{d-1} = X_{d-1} / Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2 / 4yZ_{d-1}Z_{d+1}Z_d^2 \quad \cdots \text{数 } 3 \ 1$$

- 15 $x_d = X_d / Z_d$ であるが、逆元演算の回数を減らす目的で y_d の分母と通分することにより、

$$x_d = \frac{4yZ_{d+1}Z_{d-1}Z_d X_d}{4yZ_{d+1}Z_{d-1}Z_d Z_d} \quad \cdots \text{数 } 3 \ 2$$

となる。ここで、 x_d, y_d は図 14 で示した処理により与えられる。したがって、アフィン座標 (x_d, y_d) の値が全て復元されていることになる。

- 20 上記手順はステップ 1401、ステップ 1402、ステップ 1404、ステップ 1407、ステップ 1409、ステップ 1410、ステップ 1411、ステップ 1412、ステップ 1413、ステップ 1415 及びステップ 1416 において有限体上の乗算の計算量を必要とする。ただし、ステップ 1408 の乗算は、被乗数の値が 4 と小さいので、その計算量は通常の乗算の計算量と比べて小さい
- 25 為無視してよい。また、ステップ 1406 において有限体上の 2 乗算の計算量を必要とする。また、ステップ 1414 において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の

乗算の計算量を M 、有限体上の2乗算の計算量を S 及び有限体上の逆元演算の計算量を I とすると、上記手順は $11M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500 M 弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は51.8 M であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた x_d, y_d の値が計算できれば x_d, y_d の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。

次に図7により、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部202では、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P を入力し、以下の手順によりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ のうち X_{d-1} 及び Z_{d-1} を出力する。ステップ716として、与えられたワイエルシュトラス型楕円曲線上の点 P をモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点 P とする。ステップ701として、変数 I に初期値1を代入する。ステップ702として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点 $2P$ を計算する。ステップ703として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ702で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ704として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すればステップ714へ行く。一致しなければステップ7

- 05へ行く。ステップ705として、変数Iを1増加させる。ステップ706として、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ707へ行く。そのビットの値が1であればステップ710へ行く。ステップ707として、射影座標により表された点の組
- 5 (mP, (m+1)P) から点mPと点(m+1)Pの加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ708へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ708として、射影座標により表された点の組(mP, (m+1)P) から点mPの2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ709へ行く。ここで、2倍算 $2(mP)$ は、モン
- 10 ギョメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ709として、ステップ708で求めた点 $2mP$ とステップ707で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ704へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ710として、射影
- 15 座標により表された点の組(mP, (m+1)P) から点mPと点(m+1)Pの加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ711へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ711として、射影座標により表された点の組(mP, (m+1)P) から点(m+1)Pの2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステッ
- 20 プ712へ行く。ここで、2倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ712として、ステップ710で求めた点 $(2m+1)P$ とステップ711で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ704へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、点mP及び点(m+1)Pは全て射
- 25 影座標において表されている。ステップ714として、射影座標で表された点の組(mP, (m+1)P) から、点(m-1)Pの射影座標におけるX座標 X_{m-1} 及びZ座標 Z_{m-1} を求める。その後ステップ715へ行く。ステップ715として、モンゴメリ型楕円曲線における点(m-1)Pを、ワイエルシュトラス型楕円曲線上で射影座標により表された点に変換する。その点のX座標及びZ座標をそれぞれあらためて

- X_{m-1} 及び Z_{m-1} とおく。また、モンゴメリ型楕円曲線において射影座標で表された点の組 $(mP, (m+1)P)$ に対して、点 mP 及び点 $(m+1)P$ をワイエルシュトラス型楕円曲線上で射影座標で表された点に変換し、それぞれ $mP = (X_m, Y_m, Z_m)$ 及び $(m+1)P = (X_{m+1}, Y_{m+1}, Z_{m+1})$ とあらためて置き直す。ここで、 Y_m 及び
- 5 Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び2倍算の公式では Y 座標を求める事ができないので、求まっていない。ステップ713として、ワイエルシュトラス型楕円曲線上で射影座標で表された点 $(m-1)P$ の X 座標 X_{m-1} 及び Z 座標 Z_{m-1} をそれぞれ X_{d-1} 及び Z_{d-1} として、ワイエルシュトラス型楕円曲線上で射影座標で表された点 $mP = (X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ
- 10 X_d 及び Z_d として、ワイエルシュトラス型楕円曲線上で射影座標で表された点 $(m+1)P = (X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} として、出力する。また上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ714において $(m-1)P$ を求める際に、数13、数14の公式により求めてもよい
- 15 し、 m が奇数であれば、 $((m-1)/2)P$ の値をステップ712の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の2倍算の公式より、 $(m-1)P$ を求めてもよい。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ ととることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体
- 20 上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M+2S$ である。スカラー値の I 番目のビットの値が0であれば、ステップ707において加算の計算量、ステップ708において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ710において加算の計算量、ステ
- 25 ップ711において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要である。いずれの場合においても $6M+4S$ の計算量が必要である。ステップ704、ステップ705、ステップ706、ステップ707、ステップ708、ステップ709乃至はステップ704、ステップ705、ステップ706、ステップ710、ステップ711、ステップ712の繰り返しの回数は、(スカ

ラー値 d のビット長) — 1 回となるので、ステップ 7 0 2 での 2 倍算の計算量と
 ステップ 7 1 6 でのモンゴメリ型楕円曲線上の点への変換に必要な計算量及びス
 テップ 7 1 5 でのワイエルシュトラス型楕円曲線上の点への変換に必要な計算量
 を考慮に入れると、全体の計算量は $(6M + 4S)k + 4M$ となる。ここで k は
 5 スカラー値 d のビット長である。一般的には、計算量 S は、 $S = 0.8M$ 程度と
 見積もられるので、全体の計算量はおおよそ $(9.2k + 4)M$ となる。例えば
 スカラー値 d が 1 6 0 ビット ($k = 160$) であれば、上記手順のアルゴリズム
 の計算量はおおよそ 1 4 7 6 M となる。スカラー値 d のビットあたりの計算量と
 してはおおよそ 9.2 M となる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic
 10 curve exponentiation using mixed coordinates, Advances in Cryptology
 Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシ
 ュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とし
 た混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記
 載されている。この場合においては、スカラー値のビットあたりの計算量はおお
 15 よそ 1 0 M と見積もられる。例えばスカラー値 d が 1 6 0 ビット ($k = 160$)
 であれば、このスカラー倍計算方法の計算量はおおよそ 1 6 0 0 M となる。した
 がって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部 2 0 2 において上記手順のアルゴリズムを用いなく
 ても、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d,$
 20 $X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムであり且つ高速であれ
 ば、他のアルゴリズムを用いてもよい。

スカラー倍計算部 1 0 3 における座標復元部 2 0 3 の座標復元に必要な計算量
 は $11M + S + I$ であり、これは高速スカラー倍計算部 2 0 2 の高速スカラー倍
 計算に必要な計算量の $(9.2k + 4)M$ とに比べてはるかに小さい。したがっ
 25 て、スカラー倍計算部 1 0 3 のスカラー倍計算に必要な計算量は、高速スカラー
 倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M,$
 $S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 55.8)M$ と
 見積もることができる。例えばスカラー値 d が 1 6 0 ビット ($k = 160$) であ
 れば、このスカラー倍計算に必要な計算量はおおよそ 1 5 2 8 M となる。楕円曲

線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおよそ1640Mであり、これと比べて必要となる計算量は削減されている。

- 5 第7の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部103の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部103の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部103
- 10 がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部103に入力すると高速スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部202は受け取ったスカラー値 d と
- 15 与えられたワイエルシュトラス型楕円曲線上の点 P からワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部203に与える。
- 20 座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}, x$ 及び y よりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標 X_d, Y_d 及び Z_d の復元を行なう。スカラー
- 25 倍計算部103は射影座標において完全に座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算結果として出力する。

次に図15により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ が与えられた場合に X_d, Y_d, Z_d を出力する座標復元部の処理について説明する。

座標復元部203では、ワイエルシュトラス型楕円曲線において射影座標で表

- されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} 、スカラー倍計算部 103 に入力されたワイエルシュトラス型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順で射影座標において完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてワイエルシュトラス型楕円曲線に
- 10 おけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。
- 15 ステップ 1501 において $X_{d-1} \times Z_{d+1}$ が計算され、 T_1 に格納される。ステップ 1502 において $Z_{d-1} \times X_{d+1}$ が計算され、 T_2 に格納される。ステップ 1503 において $T_1 - T_2$ が計算される。ここで T_1 には $X_{d-1}Z_{d+1}$ が T_2 には $Z_{d-1}X_{d+1}$ がそれぞれ格納されており、したがって $X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1}$ が計算される。その結果が T_1 に格納される。ステップ 1504 において
- 20 $Z_d \times x$ が計算され、 T_2 に格納される。ステップ 1505 において $X_d - T_2$ が計算される。ここで T_2 には $Z_d x$ が格納されており、したがって $X_d - xZ_d$ が計算される。その結果が T_2 に格納される。ステップ 1506 において T_2 の 2 乗が計算される。ここで T_2 には $X_d - xZ_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果が T_2 に格納される。ステップ 1507 において $T_1 \times T_2$
- 25 が計算される。ここで T_1 には $X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1}$ が T_2 には $(X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $(X_d - xZ_d)^2 (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ が計算される。その結果がレジスタ Y_d に格納される。ステップ 1508 において $4 \times y$ が計算される。その結果が T_2 に格納される。ステップ 1509 において $T_2 \times Z_{d+1}$ が計算される。ここで T_2 には $4y$ が格納されており、したが

- って $4yZ_{d+1}$ が計算される。その結果が T_2 に格納される。ステップ 1 5 1 0 において $T_2 \times Z_{d-1}$ が計算される。ここで T_2 には $4yZ_{d+1}$ が格納されており、したがって $4yZ_{d+1}Z_{d-1}$ が計算される。その結果が T_2 に格納される。ステップ 1 5 1 1 において $T_2 \times Z_d$ が計算される。ここで T_2 には $4yZ_{d+1}Z_{d-1}$ が格納されており、したがって $4yZ_{d+1}Z_{d-1}Z_d$ が計算される。その結果が T_2 に格納される。ステップ 1 5 1 2 において $T_2 \times X_d$ が計算される。ここで T_2 には $4yZ_{d+1}Z_{d-1}Z_d$ が格納されており、したがって $4yZ_{d+1}Z_{d-1}Z_dX_d$ が計算される。その結果がレジスタ X_d に格納される。ステップ 1 5 1 3 において $T_2 \times Z_d$ が計算される。ここで T_2 には $4yZ_{d+1}Z_{d-1}Z_d$ が格納されており、したがって $4yZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果がレジスタ Z_d に格納される。したがってレジスタ Z_d には $4yZ_{d+1}Z_{d-1}Z_dZ_d$ が格納されている。レジスタ Y_d にはステップ 1 5 0 7 において $(X_d - xZ_d)^2(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ が格納され、その後更新が行われないので、その値が保持されている。レジスタ X_d にはステップ 1 5 1 2 において $4yZ_{d+1}Z_{d-1}Z_dX_d$ が格納され、その後更新が行われないので、その値が保持されている。

- 上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 X_{d-1} 、 Z_{d-1} からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標 (X_d, Y_d, Z_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数 2 7、数 2 8 を得る。両辺を各々減算することにより、数 2 9 を得る。したがって、数 3 0 となる。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ 、 $x_{d-1} = X_{d-1}/Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、数 3 1 を得る。 $x_d = X_d/Z_d$ であるが、 y_d の分母と通分することにより、数 3 2 となる。

その結果として

$$Y_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_dx)^2 \quad \cdots \text{数 3 3}$$

とし、 X_d 及び Z_d をそれぞれ

$$4yZ_{d+1}Z_{d-1}Z_dX_d \quad \cdots \text{数 3 4}$$

$4y_{Z_{d+1}Z_{d-1}Z_dZ_d} \dots$ 数 3 5

により更新すればよい。

ここで、 X_d , Y_d , Z_d は図15で示した処理により与えられる。したがって、射影座標(X_d, Y_d, Z_d)の値は全て復元されたことになる。

- 5 上記手順はステップ1501、ステップ1505、ステップ1504、ステップ1507、ステップ1509、ステップ1510、ステップ1511、ステップ1512及びステップ1513において有限体上の乗算の計算量を必要とする。
- ただし、ステップ1508の乗算は、被乗数の値が4と小さいので、その計算量は通常の乗算の計算量と比べて小さい為無視してよい。また、ステップ150
- 10 6において有限体上の2乗算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、2乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の2乗算の計算量をSとすると、上記手順は $9M + S$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが160ビットであれば、高速ス
- 15 calar倍計算の計算量はおおよそ1500M弱と見積もられる。S=0.8Mと仮定すると座標復元の計算量は9.8Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

- 尚、上記手順をとらなくても、上記計算式により与えられた X_d, Y_d, Z_d の値が
- 20 計算できれば X_d, Y_d, Z_d の値が復元できる。また、 x_d, y_d が上記計算式により与えられる値を取るように X_d, Y_d, Z_d の値を選択し、その値が計算できれば X_d, Y_d, Z_d が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。

- 次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、 $X_d, Z_d,$
- 25 $X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムについて説明する。

第7実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、第6実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。

尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくても、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- 5 スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $9M + S$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 4)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ と仮定
- 10 すると、この計算量はおよそ $(9.2k + 13.8)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量はおよそ 1486M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン
- 15 座標として出力する場合に必要な計算量はおよそ 1600M であり、これと比べて必要となる計算量は削減されている。

- 第 8 の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部 103 の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部 103 の内部の計算で
- 20 使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部 103 がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円
- 25 曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P =$

(x_{d+1}, y_{d+1})の座標のうち x_{d+1} 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ の座標のうち x_{d-1} を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部203に与える。座標復元部203は与えられた座標の値 x_d, x_{d+1}, x_{d-1}, x 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 y_d の復元を行なう。スカラー倍計算部103はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。

次に図16により、座標 $x, y, x_d, x_{d+1}, x_{d-1}$ が与えられた場合に、 x_d, y_d を出力する座標復元部の処理について説明する。

座標復元部203では、ワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ の座標のうち x_{d-1} 、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。

ステップ1601において $x_d - x$ が計算され、 T_1 に格納される。ステップ1602において T_1 の2乗すなわち $(x_d - x)^2$ が計算され、 T_1 に格納される。ステップ1603において $x_{d-1} - x_{d+1}$ が計算され、 T_2 に格納される。ステップ1604において $T_1 \times T_2$ が計算される。ここで T_1 には $(x_d - x)^2$ が T_2 には $x_{d-1} - x_{d+1}$ がそれぞれ格納されており、したがって $(x_d - x)^2 (x_{d-1} - x_{d+1})$ が計算される。その結果が T_1 に格納される。ステップ1605において $4 \times y$ が計算され、 T_2 に格納される。ステップ1606において T_2 の逆元が計算される。ここで T_2 には $4y$ が格納されており、したがって $1/4y$ が計算される。その結果が T_2 に格納される。ステップ1607において $T_1 \times T_2$ が計算される。ここで T_1 には $(x_d - x)^2 (x_{d-1} - x_{d+1})$ が T_2 には $1/4y$ がそれぞれ格納されており、したがって $(x_d - x)^2 (x_{d-1} - x_{d+1}) / 4y$ が計算される。その結果が

レジスタ y_d に格納される。したがってレジスタ y_d には $(x_d - x)^2 (x_{d-1} - x_{d+1})/4y$ が格納されている。レジスタ x_d は全く更新されないので入力された値が保持されている。

上記手順によりスカラー倍点の y 座標 y_d が復元される理由は以下の通りである。

- 5 点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数27、数28を得る。両辺を各々減算することにより、数29を得る。したがって、数30となる。ここで x_d, y_d は図16の処理によって与えられる。したがって、アフィン座標 (x_d, y_d) の値を全て復元していることになる。
- 10 上記手順はステップ1604、ステップ1607において有限体上の乗算の計算量を必要とする。ただし、ステップ1605の乗算は、被乗数の値が4と小さいので、その計算量は通常の乗算の計算量と比べて小さい為無視してよい。また、ステップ1602において有限体上の2乗算の計算量を必要とする。さらにステップ1606において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、2乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の2乗算の計算量を S 、有限体上の逆元演算の計算量を I とすると、上記手順は $2M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が160ビットであれば、高速スカラー倍計算の計算量はおよそ1500 M 弱と見積もられる。 $S = 0.8M$ 及び $I = 40M$ と仮定すると座標復元の計算量は42.8 M であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。
- 20

- 尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば y_d の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。
- 25

次に図7により、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 x_d, x_{d+1}, x_{d-1} を出力するアルゴリズムについて説明する。

高速スカラー倍計算部202では、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P を入力し、以下の手順によりワイエルシュト

- ラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ のうち x_d 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ のうち x_{d+1} 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ のうち x_{d-1} を出力する。ステップ
- 5 716として、与えられたワイエルシュトラス型楕円曲線上の点 P をモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点 P とする。ステップ701として、変数 I に初期値1を代入する。ステップ702として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍
- 10 点 $2P$ を計算する。ステップ703として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ702で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ704として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すれば $m=d$ となり、ステップ714へ行く。一致しなければステップ705へ行く。ステップ
- 15 705として、変数 I を1増加させる。ステップ706として、スカラー値の I 番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ707へ行く。そのビットの値が1であればステップ710へ行く。ステップ707として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ70
- 20 8へ行く。ここで、加算 $mP + (m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ708として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ709へ行く。ここで、2倍算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ709として、ステ
- 25 ュップ708で求めた点 $2mP$ とステップ707で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ704へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ710として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+$

- 1) Pを計算する。その後ステップ7 1 1へ行く。ここで、加算 $mP + (m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ7 1 1として、射影座標により表された点の組(mP , $(m+1)P$)から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ7 1 2へ行く。
- 5 ここで、2倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ7 1 2として、ステップ7 1 0で求めた点 $(2m+1)P$ とステップ7 1 1で求めた点 $(2m+2)P$ を点の組($(2m+1)P$, $(2m+2)P$)として、点の組(mP , $(m+1)P$)の代わりに格納する。その後ステップ7 0 4へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。
- 10 ステップ7 1 4として、射影座標で表された点の組(mP , $(m+1)P$)から、点 $(m-1)P$ の射影座標におけるX座標 x_{m-1} 及びZ座標 z_{m-1} を求める。その後ステップ7 1 5へ行く。ステップ7 1 5として、モンゴメリ型楕円曲線における点 $(m-1)P$ を、ワイエルシュトラス型楕円曲線上でアフィン座標により表された点に変換する。その点のx座標をそれぞれあらためて x_{m-1} とおく。また、モンゴメリ型楕円
- 15 曲線において射影座標で表された点の組(mP , $(m+1)P$)に対して、点 mP 及び点 $(m+1)P$ をワイエルシュトラス型楕円曲線上でアフィン座標で表された点に変換し、それぞれ $mP = (x_m, y_m)$ 及び $(m+1)P = (x_{m+1}, y_{m+1})$ とあらためて置き直す。ここで、 y_m 及び y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び2倍算の公式ではY座標を求める事ができないので、求まっていない。その後ステップ
- 20 プ7 1 3へ行く。ステップ7 1 3として、ワイエルシュトラス型楕円曲線上でアフィン座標で表された点 $(m-1)P$ のx座標 x_{m-1} を x_{d-1} として、ワイエルシュトラス型楕円曲線上で射影座標で表された点 $mP = (x_m, y_m)$ より x_m を x_d として、ワイエルシュトラス型楕円曲線上でアフィン座標で表された点 $(m+1)P = (x_{m+1}, y_{m+1})$ より x_{m+1} を x_{d+1} として、出力する。また上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ7 1 4において $(m-1)P$ を求める際に、数1 3、数1 4の公式により求めてもよいし、 m が奇数であれば、 $((m-1)/2)P$ の値をステップ7 1 2の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の2倍算の公式より、 $(m-1)P$ を求めてもよい。
- 25

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1 = 1$ とすることにより $3M + 2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M + 2S$ である。スカラー値の I 番目のビットの値が0であれば、ステップ707において加算の計算量、ステップ708において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ710において加算の計算量、ステップ711において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要である。いずれの場合においても $6M + 4S$ の計算量が必要である。ステップ704、ステップ705、ステップ706、ステップ707、ステップ708、ステップ709乃至はステップ704、ステップ705、ステップ706、ステップ710、ステップ711、ステップ712の繰り返しの回数は、(スカラー値 d のビット長) $- 1$ 回となるので、ステップ702での2倍算の計算量とステップ716でのモンゴメリ型楕円曲線上への点への変換に必要な計算量及びステップ715でのワイエルシュトラス型楕円曲線上の点への必要な計算量を考慮に入れると、全体の計算量は $(6M + 4S)k + 15M + I$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S = 0.8M$ 程度、計算量 I は、 $I = 40M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k + 55)M$ となる。例えばスカラー値 d が160ビット ($k = 160$) であれば、上記手順のアルゴリズムの計算量はおおよそ $1527M$ となる。スカラー値 d のビットあたりの計算量としてはおおよそ $9.2M$ となる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ $10M$ と見積もられる。例えばスカラー値 d が160ビット ($k = 160$) であれば、このスカラー倍計算方法の計算量はおおよそ $1640M$ となる。したがって、上記手順のアルゴリズムの方が計算量が少

なく高速といえる。

尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 x_d ,

x_{d+1}, x_{d-1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $2M + S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 55)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M$ 、 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 97.8)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量は 1570M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおよそ 1640M であり、これと比べて必要となる計算量は削減されている。

第 9 の実施例は、入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部 103 がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものである。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算する。また、入力されたワ

- イエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たに $P=(x, y)$ とおく。高速スカラー倍計算部 202 は、 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値
- 5 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP=(x_d, y_d)$ の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部 103 はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。

- 次に図 17 により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に x_d, y_d
- 10 を出力する座標復元部の処理について説明する。

- 座標復元部 203 では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ の座標うち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部 103 に入力されたモンゴメリ型楕円曲線上の点Pを
- 15 アフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d^{Mon}, y_d^{Mon}) で、射影座標を $(X_d, Y_d,$
- 20 $Z_d)$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- ステップ 1701 において $X_d \times x$ が計算され、レジスタ T_1 に格納される。ス
- 25 テップ 1702 において $T_1 - Z_d$ が計算される。ここでレジスタ T_1 には $X_d x$ が格納されており、したがって $X_d x - Z_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 1703 において $Z_d \times x$ が計算され、レジスタ T_2 に格納される。ステップ 1704 において $X_d - T_2$ が計算される。ここでレジスタ T_2 には $Z_d x$ が格納されており、したがって $X_d - x Z_d$ が計算される。その結果がレジ

- スタ T_2 に格納される。ステップ 1705 において $X_{d+1} \times T_2$ が計算される。ここでレジスタ T_2 には $X_d - xZ_d$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 1706 において T_2 の 2 乗が計算される。ここでレジスタ T_2 には $(X_d - xZ_d)$ が格納されてお
- 5 り、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1707 において $T_2 \times X_{d+1}$ が計算される。ここでレジスタ T_2 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1708 において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $X_{d+1} (X_d - xZ_d)^2$ が格納されており、
- 10 したがって $Z_{d+1} X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1709 において $T_2 \times y$ が計算される。ここでレジスタ T_2 には $Z_{d+1} X_{d+1} (X_d - xZ_d)^2$ が格納されており、したがって $yZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1710 において $T_2 \times B$ が計算される。ここでレジスタ T_2 には $yZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が格納されてお
- 15 り、したがって $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1711 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2$ が格納されており、したがって $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1712 において $T_2 \times X_d$ が計算される。
- 20 ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が格納されており、したがって $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d X_d$ が計算される。その結果がレジスタ T_4 に格納される。ステップ 1713 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が格納されており、したがって $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が計算される。その結果がレジスタ T_2 に格納さ
- 25 れる。ステップ 1714 においてレジスタ $T_2 \times s$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が格納されており、したがって $sByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1715 において T_2 の逆元が計算される。ここで、 T_2 には $sByZ_{d+1} X_{d+1} (X_d - xZ_d)^2 Z_d$ が格納されており、したがって $1 / sByZ_{d+1}$

$X_{d+1}(X_d - xZ_d)^2 Z_d^2$ が計算される。その結果が T_2 に格納される。ステップ 1 7 1 6において $T_2 \times T_4$ が計算される。ここでレジスタ T_2 には $1/sByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d^2$ がレジスタ T_4 には $ByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d X_d$ がそれぞれ格納されており、したがって $(ByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d X_d) /$

- 5 $(sByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d^2)$ が計算される。その結果がレジスタ T_4 に格納される。ステップ 1 7 1 7において $T_4 + \alpha$ が計算される。ここでレジスタ T_4 には $(ByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d X_d) / (sByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d^2)$ が格納されており、従って、数 3 6が計算される。

$$\frac{ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 X_d}{sByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d} + \alpha \quad \cdots \text{数 3 6}$$

- 10 その結果が、レジスタ x_d に格納される。ステップ 1 7 1 8において $T_1 \times Z_{d+1}$ が計算される。ここでレジスタ T_1 には $X_d x - Z_d$ が格納されており、したがって $Z_{d+1}(X_d x - Z_d)$ が計算される。その結果がレジスタ T_4 に格納される。ステップ 1 7 1 9においてレジスタ T_1 の2乗が計算される。ここでレジスタ T_1 には $(X_d x - Z_d)$ が格納されており、したがって $(X_d x - Z_d)^2$ が計算される。その結果が
- 15 レジスタ T_1 に格納される。ステップ 1 7 2 0において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(X_d x - Z_d)^2$ がレジスタ T_2 には $1/sByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d^2$ がそれぞれ格納されており、したがって $(X_d x - Z_d)^2 / sByZ_{d+1} X_{d+1}(X_d - xZ_d)^2 Z_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1 7 2 1において $T_3 + T_4$ が計算される。ここでレジスタ T_3 には
- 20 $X_{d+1}(X_d - xZ_d)$ がレジスタ T_4 には $Z_{d+1}(X_d x - Z_d)$ がそれぞれ格納されており、したがって $X_{d+1}(X_d - xZ_d) + Z_{d+1}(X_d x - Z_d)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 1 7 2 2において $T_3 - T_4$ が計算される。ここでレジスタ T_3 には $X_{d+1}(X_d - xZ_d)$ がレジスタ T_4 には $Z_{d+1}(X_d x - Z_d)$ がそれぞれ格納されており、したがって $X_{d+1}(X_d - xZ_d) - Z_{d+1}(X_d x - Z_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 1 7 2 3において $T_1 \times$
- 25 T_3 が計算される。ここでレジスタ T_1 には $X_{d+1}(X_d - xZ_d) + Z_{d+1}(X_d x - Z_d)$ がレジスタ T_3 には $X_{d+1}(X_d - xZ_d) - Z_{d+1}(X_d x - Z_d)$ がそれぞれ格納されており、したがって $\{X_{d+1}(X_d - xZ_d) + Z_{d+1}(X_d x - Z_d)\} \{X_{d+1}(X_d - xZ_d) - Z_{d+1}(X_d x -$

$Z_d\}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 1 7 2 4
 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $\{X_{d+1}(X_d - xZ_d) + Z_{d+1}(X_d x - Z_d)\}$ $\{X_{d+1}(X_d - xZ_d) - Z_{d+1}(X_d x - Z_d)\}$ がレジスタ T_2 には $(X_d x - Z_d)^2 / sByZ_{d+1}X_{d+1}(X_d - xZ_d)^2 Z_d^2$ がそれぞれ格納されており、したがって

$$5 \quad \frac{\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}\{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2}{sByZ_{d+1}X_{d+1}(X_d - xZ_d)^2 Z_d^2}$$

… 数 3 7

が計算される。その結果がレジスタ y_d に格納される。したがってレジスタ y_d
 には数 3 7 の値が格納されている。レジスタ x_d にはステップ 1 7 1 7 において
 数 3 6 の値が格納され、その後更新が行なわれないので、その値が保持されてい
 10 る。その結果として、ワイエルシュトラス型楕円曲線におけるアフィン座標
 (x_d, y_d) の値が全て復元されている。

上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} からワイエルシ
 ュトラス型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における
 値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した
 15 点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線
 のアフィン座標における加算公式に代入すると、次の式を得る。

$$(A + x + x_d^{Mon} + x_{d+1})(x_d^{Mon} - x)^2 = B(y_d^{Mon} - y)^2 \quad \cdots \text{数 3 8}$$

$$(A + x + x_d^{Mon} + x_{d-1})(x_d^{Mon} - x)^2 = B(y_d^{Mon} + y)^2 \quad \cdots \text{数 3 9}$$

両辺を各々減算することにより、

$$20 \quad (x_{d-1} - x_{d+1})(x_d^{Mon} - x)^2 = 4By_d^{Mon}y \quad \cdots \text{数 4 0}$$

を得る。したがって、

$$y_d^{Mon} = (x_{d-1} - x_{d+1})(x_d^{Mon} - x)^2 / 4By \quad \cdots \text{数 4 1}$$

となる。ここで $x_d^{Mon} = X_d / Z_d$ 、 $x_{d+1} = X_{d+1} / Z_{d+1}$ 、 $x_{d-1} = X_{d-1} / Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、次
 25 の式を得る。

$$y_d^{Mon} = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2 / 4ByZ_{d-1}Z_{d+1}Z_d^2 \quad \cdots \text{数 4 2}$$

モンゴメリ型楕円曲線の射影座標での加算公式は既を示した数 1 1、数 1 2 であ
 る。ここで X_m 及び Z_m はモンゴメリ型楕円曲線上の点 P の m 倍点 mP の射影座標に

- におけるX座標及びZ座標、 X_n 及び Z_n はモンゴメリ型楕円曲線上の点Pの n 倍点 nP の射影座標におけるX座標及びZ座標、 X_{m-n} 及び Z_{m-n} はモンゴメリ型楕円曲線上の点Pの $(m-n)$ 倍点 $(m-n)P$ の射影座標におけるX座標及びZ座標、 X_{m+n} 及び Z_{m+n} はモンゴメリ型楕円曲線上の点Pの $(m+n)$ 倍点 $(m+n)P$ の射影座標におけるX座標及びZ座標であり、 m, n は $m > n$ をみたす正整数である。この式は $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m-n}/Z_{m-n} = x_{m-n}$ が不変のとき、 $X_{m+n}/Z_{m+n} = x_{m+n}$ も不変となるので、射影座標での公式としてうまく働いている。他方、数13、数14とおくと、この式も $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m-n}/Z_{m-n} = x_{m-n}$ が不変のとき、 $X_{m+n}/Z_{m+n} = x_{m-n}$ も不変となる。また、 $X'_{m-n}/Z'_{m-n} = X_{m-n}/Z_{m-n} = x_{m-n}$ をみたすので、 x_{m-n} の射影座標として X'_{m-n}, Z'_{m-n} をとってよい。 $m=d, n=1$ として上記公式を用いて y_d^{Mon} の式より X_{d-1} 及び Z_{d-1} を消去し、 $X_1=x, Z_1=1$ とおくことにより、次の式を得る。

$$y_d^{Mon} = \frac{\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - x Z_d)\} \{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - x Z_d)\} (X_d x - Z_d)^2}{ByZ_{d+1}X_{d+1}(X_d - x Z_d)^2 Z_d^2}$$

15

… 数 4 3

$x_d^{Mon} = X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d^{Mod} の分母と通分することにより、

$$x_d^{Mon} = \frac{ByZ_{d+1}X_{d+1}Z_d(X_d - x Z_d)^2 X_d}{ByZ_{d+1}X_{d+1}Z_d(X_d - x Z_d)^2 Z_d} \quad \dots \text{数 4 4}$$

- となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタを s, α として、 $y_d = s - ly_d^{Mon}$ 及び $x_d = s - lx_d^{Mon} + \alpha$ の関係がある。結果として数45、数46を得る。

$$y_d = \frac{\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - x Z_d)\} \{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - x Z_d)\} (X_d x - Z_d)^2}{sByZ_{d+1}X_{d+1}(X_d - x Z_d)^2 Z_d^2}$$

… 数 4 5

$$x_d = (ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 X_d) / (sByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 Z_d) + \alpha$$

… 数 4 6

ここで、 x_d, y_d は図 1 7 より与えられる。したがって、ワイエルシュトラス型楕円曲線におけるアフィン座標 (x_d, y_d) の値が全て復元されていることになる。

上記手順はステップ 1 7 0 1、ステップ 1 7 0 3、ステップ 1 7 0 5、ステップ 1 7 0 7、ステップ 1 7 0 8、ステップ 1 7 0 9、ステップ 1 7 1 0、ステップ 1 7 1 1、ステップ 1 7 1 2、ステップ 1 7 1 3、ステップ 1 7 1 4、ステップ 1 7 1 6、ステップ 1 7 1 8、ステップ 1 7 2 0、ステップ 1 7 2 3 及びステップ 1 7 2 4 において有限体上の乗算の計算量を必要とする。また、ステップ 1 7 0 6 及びステップ 1 7 1 9 において有限体上の 2 乗算の計算量を必要とする。また、ステップ 1 7 1 5 において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S 及び有限体上の逆元演算の計算量を I とすると、上記手順は $16M + 2S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 1 6 0 ビットであれば、高速スカラー倍計算の計算量はおおよそ 1 5 0 0 M 弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は 5 7. 6 M であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた x_d, y_d の値が計算できれば x_d, y_d の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタである B の値やモンゴメリ型楕円曲線への変換パラメタである s を小さくすることにより、ステップ 1 7 1 0 における乗算の計算量やステップ 1 7 1 4 における乗算の計算量を削減することができる。

次に図 8 により、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力する高速スカラー倍計算部の処理について説明

する。

- 高速スカラー倍計算部 202 では、スカラー倍計算部 103 に入力されたワイエルシュトラス型楕円曲線上の点 P を入力し、以下の手順によりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ のうち X_d 及び
- 5 Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ のうち X_{d+1} 及び Z_{d+1} を出力する。ステップ 816 として、与えられたワイエルシュトラス型楕円曲線上の点 P をモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点 P とする。ステップ 801 として、変数 I に初期値 1 を代入する。ステップ 802 として、点 P の 2 倍点 $2P$
- 10 を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて 2 倍点 $2P$ を計算する。ステップ 803 として、スカラー倍計算部 103 に入力された楕円曲線上の点 P とステップ 802 で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ 804 として、変数 I とスカラー値 d のビット
- 15 ト長とが一致するかどうかを判定し、一致すればステップ 813 へ行く。一致しなければステップ 805 へ行く。ステップ 805 として、変数 I を 1 増加させる。ステップ 806 として、スカラー値の I 番目のビットの値が 0 であるか 1 であるかを判定する。そのビットの値が 0 であればステップ 807 へ行く。そのビットの値が 1 であればステップ 810 へ行く。ステップ 807 として、射影座標により
- 20 表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 808 へ行く。ここで、加算 $mP + (m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ 808 として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の 2 倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ 809 へ行く。ここで、2 倍
- 25 算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算される。ステップ 809 として、ステップ 808 で求めた点 $2mP$ とステップ 807 で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 804 へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ 810 として、

- 射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)$ を計算する。その後ステップ 8 1 1 へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ 8 1 1 として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の 2 倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ 8 1 2 へ行く。ここで、2 倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算される。ステップ 8 1 2 として、ステップ 8 1 0 で求めた点 $(2m+1)P$ とステップ 8 1 1 で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 8 0 4 へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ 8 1 3 として、射影座標で表された点の組 $(mP, (m+1)P)$ から、射影座標で表された点 $mP=(X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d として、射影座標で表された点 $(m+1)P=(X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} として、出力する。ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び 2 倍算の公式では Y 座標を求める事ができないので、求まっていない。また上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ ととることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の 2 乗算の計算量である。モンゴメリ型楕円曲線の射影座標における 2 倍算の公式の計算量は、 $3M+2S$ である。スカラー値の I 番目のビットの値が 0 であれば、ステップ 8 0 7 において加算の計算量、ステップ 8 0 8 において 2 倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が 1 であれば、ステップ 8 1 0 において加算の計算量、ステップ 8 1 1 において 2 倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要である。いずれの場合においても $6M+4S$ の計算量が必要である。ステップ 8 0 4、ステップ 8 0 5、ステップ 8 0 6、ステップ 8 0 7、ステップ 8 0 8、ステップ 8 0 9 乃至はステップ 8 0 4、ステップ 8 0 5、ステップ 8 0 6、ステ

- ステップ810、ステップ811、ステップ812の繰り返しの回数は、(スカラー値 d のビット長) - 1回となるので、ステップ802での2倍算の計算量及びステップ816でのモンゴメリ型楕円曲線上の点への変換の計算量を考慮に入れると、全体の計算量は $(6M + 4S)(k - 1) + 4M + 2S$ となる。ここで k は
- 5 スカラー値 d のビット長である。一般的には、計算量 S は、 $S = 0.8M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k - 3.6)M$ となる。例えばスカラー値 d が160ビット ($k = 160$) であれば、上記手順のアルゴリズムの計算量はおおよそ1468Mとなる。スカラー値 d のビットあたりの計算量としてはおおよそ9.2Mとなる。A.Miyaji, T.Ono, H.Cohen, Efficient
- 10 elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp.51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計
- 15 算量はおおよそ10Mと見積もられる。例えばスカラー値 d が160ビット ($k = 160$) であれば、このスカラー倍計算方法の計算量はおおよそ1600Mとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。
- 尚、高速スカラー倍計算部202において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d,$
- 20 X_{d+1}, Z_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。
- スカラー倍計算部103における座標復元部203の座標復元に必要な計算量は $16M + 2S + I$ であり、これは高速スカラー倍計算部202の高速スカラー倍計算に必要な計算量の $(9.2k - 3.6)M$ とに比べてはるかに小さい。し
- 25 たがって、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M, S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 54)M$ と見積もることができる。例えばスカラー値 d が160ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量は1526Mとなる。楕円曲線とし

てワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおよそ1640Mであり、これと比べて必要となる計算量は削減されている。

- 5 第10の実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部103がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点,
- 10 (X_d^W, Y_d^W, Z_d^W) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部103に入力すると高速スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部202は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ の座標のうち X_d 及び
- 15 Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点 P を、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たに $P=(x, y)$ とおく。高速スカラー倍計算部202は、 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$
- 20 及び y を座標復元部203に与える。座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d^W, Y_d^W, Z_d^W)$ の座標 X_d^W, Y_d^W 及び Z_d^W の復元を行なう。スカラー倍計算部103は射影座標において完全に座標が与えられたスカラー倍点 (X_d^W, Y_d^W, Z_d^W) を計算結果として出力する。
- 25 次に図18により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に X_d^W, Y_d^W, Z_d^W を出力する座標復元部の処理について説明する。

座標復元部203では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び

- Z_{d+1} 、スカラー倍計算部 103 に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でワイエルシュトラス型楕円曲線上で射影座標において完全な座標が与えられたスカラー倍点 (X_d^W, Y_d^W, Z_d^W) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン
- 5 座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を
- 10 (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。
- ステップ 1801 において $X_d \times x$ が計算され、レジスタ T_1 に格納される。ステップ 1802 において $T_1 - Z_d$ が計算される。ここでレジスタ T_1 には $X_d x$ が格納されており、したがって $X_d x - Z_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 1803 において $Z_d \times x$ が計算され、レジスタ T_2 に格納
- 15 される。ステップ 1804 において $X_d - T_2$ が計算される。ここでレジスタ T_2 には $Z_d x$ が格納されており、したがって $X_d - xZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1805 において $Z_{d+1} \times T_1$ が計算される。ここでレジスタ T_1 には $X_d x - Z_d$ が格納されており、したがって $Z_{d+1} (X_d x - Z_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 1806 において
- 20 $X_{d+1} \times T_2$ が計算される。ここでレジスタ T_2 には $X_d - xZ_d$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)$ が計算される。その結果がレジスタ T_4 に格納される。ステップ 1807 において T_1 の 2 乗が計算される。ここでレジスタ T_1 には $X_d x - Z_d$ が格納されており、したがって $(X_d x - Z_d)^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 1808 において T_2 の 2 乗が計算
- 25 される。ここでレジスタ T_2 には $X_d - xZ_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1809 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $(X_d - xZ_d)^2$ が格納されており、したがって $Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1810 において $T_2 \times X_{d+1}$ が計算される。ここでレジ

- スタ T_2 には $Z_d (X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1811 において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が計算される。その結果
- 5 がレジスタ T_2 に格納される。ステップ 1812 において $T_2 \times y$ が計算される。ここでレジスタ T_2 には $Z_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $yZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1813 において $T_2 \times B$ が計算される。ここでレジスタ T_2 には $yZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $ByZ_{d+1} X_{d+1}$
- 10 $Z_d (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1814 において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 X_d$ が計算される。その結果がレジスタ T_5 に格納される。ステップ 1815 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2$ が格納されており、したがって $ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d$ が
- 15 計算される。その結果がレジスタ T_2 に格納される。ステップ 1816 において $T_2 \times s$ が計算される。ここでレジスタ T_2 には $ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d$ が格納されており、したがって $sByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d$ が計算される。その結果が $Z_d W$ に格納される。ステップ 1817 において $\alpha \times Z_d W$ が計算され
- 20 る。ここで $Z_d W$ には $sByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d$ が格納されており、したがって $\alpha sByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1818 において $T_2 + T_5$ が計算される。ここでレジスタ T_2 には $\alpha sByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 Z_d$ がレジスタ T_5 には $ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 X_d$ がそれぞれ格納されており、したがって $\alpha sByZ_{d+1}$
- 25 $X_{d+1} Z_d (X_d - xZ_d)^2 Z_d + ByZ_{d+1} X_{d+1} Z_d (X_d - xZ_d)^2 X_d$ が計算される。その結果が X_d^W に格納される。ステップ 1819 において $T_3 + T_4$ が計算される。ここでレジスタ T_3 には $Z_{d+1} (X_d x - Z_d)$ がレジスタ T_4 には $X_{d+1} (X_d - xZ_d)$ が格納されており、したがって $Z_{d+1} (X_d x - Z_d) + X_{d+1} (X_d - xZ_d)$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 1820 において $T_3 - T_4$ が計

- 算される。ここでレジスタ T_3 には $Z_{d+1}(X_d x - Z_d)$ がレジスタ T_4 には $X_{d+1}(X_d - xZ_d)$ が格納されており、したがって $Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 1821 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(X_d x - Z_d)^2$ がレジスタ T_2 には $Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)$ が格納されており、したがって $\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 1822 において $T_1 \times T_3$ が計算される。ここでレジスタ T_1 には $\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$ がレジスタ T_3 には $Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)$ が格納されており、したがって $\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}\{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$ が計算される。その結果が Y_d^W に格納される。したがって Y_d^W には $\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}\{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$ が格納されている。 X_d^W にはステップ 1818 において $ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2X_d + \alpha sByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2Z_d$ が格納され、その後更新が行われないので、その値が保持されている。 X_d^W にはステップ 1816 において $sByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2Z_d$ が格納され、その後更新が行われないので、その値が保持されている。その結果として、ワイエルシュトラス型楕円曲線における射影座標 (X_d^W, Y_d^W, Z_d^W) の値が全て復元されている。

- 上記手順により与えられた $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標 (X_d^W, Y_d^W, Z_d^W) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 6、数 7 を得る。数 6、数 7 の両辺を各々減算することにより、数 8 を得る。したがって、数 9 のようになる。
- ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ 、 $x_{d-1} = X_{d-1}/Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、数 10 を得る。モンゴメリ型楕円曲線の射影座標での加算公式は数 11、数 12 である。ここで X_m 及び Z_m はモンゴメリ型楕円曲線上の点 P の m 倍点 mP の射影座標における X 座標及び Z 座標、 X_n 及び Z_n はモンゴメリ型楕円曲線上の点 P の n 倍点 nP の射影座標における X

座標及びZ座標、 X_{m-n} 及び Z_{m-n} はモンゴメリ型楕円曲線上の点Pの(m-n)倍点(m-n)Pの射影座標におけるX座標及びZ座標、 X_{m+n} 及び Z_{m+n} はモンゴメリ型楕円曲線上の点Pの(m+n)倍点(m+n)Pの射影座標におけるX座標及びZ座標であり、m、nは $m > n$ をみたす正整数である。この式は $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m-n}/Z_{m-n} = x_{m-n}$ が不変のとき、 $X_{m+n}/Z_{m+n} = x_{m+n}$ も不変となるので、射影座標での公式としてうまく働いている。他方、数13、数14とおくと、この式も $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m-n}/Z_{m-n} = x_{m-n}$ が不変のとき、 $X_{m+n}/Z_{m+n} = x_{m+n}$ も不変となる。また、 $X'_{m-n}/Z'_{m-n} = X_{m-n}/Z_{m-n} = x_{m-n}$ をみたすので、 x_{m-n} の射影座標として X'_{m-n} 、 Z'_{m-n} をとってよい。m=d, n=1として上記

- 5 $Z_{m-n} = x_{m-n}$ が不変のとき、 $X_{m+n}/Z_{m+n} = x_{m+n}$ も不変となるので、射影座標での公式としてうまく働いている。他方、数13、数14とおくと、この式も $X_m/Z_m = x_m$ 、 $X_n/Z_n = x_n$ 、 $X_{m-n}/Z_{m-n} = x_{m-n}$ が不変のとき、 $X_{m+n}/Z_{m+n} = x_{m+n}$ も不変となる。また、 $X'_{m-n}/Z'_{m-n} = X_{m-n}/Z_{m-n} = x_{m-n}$ をみたすので、 x_{m-n} の射影座標として X'_{m-n} 、 Z'_{m-n} をとってよい。m=d, n=1として上記
- 10 公式を用いて y_d の式より X_{d-1} 及び Z_{d-1} を消去し、 $X_1=x$ 、 $Z_1=1$ とおくことにより、数15を得る。 $x_d = X_d/Z_d$ であるが、 y_d の分母と通分することにより、数16となる。その結果として、

$$Y'_d = \{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\} \{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\} (X_d x - Z_d)^2$$

…数47

- 15 とし、

$$X'_d = ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 X_d \quad \cdots \text{数48}$$

$$Z'_d = ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 Z_d \quad \cdots \text{数49}$$

とすると $(X'_d, Y'_d, Z'_d) = (X_d, Y_d, Z_d)$ となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya,

- 20 H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタを $s\alpha$ として、 $Y_d^W = Y'_d$ 、 $X_d^W = X'_d + \alpha Z_d^W$ 、及び $Z_d^W = sZ'_d$ という関係がある。結果として次の式を得る。

- 25 $Y_d^W = \{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\} \{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\} (X_d x - Z_d)^2$
- …数50

$$X_d^W = ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 X_d + \alpha Z_d^W \quad \cdots \text{数51}$$

$$Z_d^W = sByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 Z_d \quad \cdots \text{数52}$$

により更新すればよい。ここで、 X_d^W, Y_d^W, Z_d^W は図18の処理により与えら

れている。したがって、ワイエルシュトラス型楕円曲線における射影座標 (X_d^W, Y_d^W, Z_d^W) の値が全て復元されていることになる。

- 上記手順はステップ1801、ステップ1803、ステップ1805、ステップ1806、ステップ1809、ステップ1810、ステップ1811、ステップ1812、ステップ1813、ステップ1814、ステップ1815、ステップ1816、ステップ1817、ステップ1821及びステップ1822において有限体上の乗算の計算量を必要とする。また、ステップ1807及びステップ1808において有限体上の2乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の2乗算の計算量をSとすると、上記手順は $15M + 2S$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500M弱と見積もられる。 $S = 0.8M$ と仮定すると座標復元の計算量は $16.6M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

- 尚、上記手順をとらなくても、上記計算式により与えられた X_d^W, Y_d^W, Z_d^W の値が計算できれば X_d^W, Y_d^W, Z_d^W の値が復元できる。また、ワイエルシュトラス型楕円曲線においてアフィン座標におけるスカラー倍点dPを $dP = (x_d^W, y_d^W)$ とすると、 x_d^W, y_d^W が上記計算式により与えられる値を取るように X_d^W, Y_d^W, Z_d^W の値を選択し、その値が計算できれば X_d^W, Y_d^W, Z_d^W が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタであるBの値やモンゴメリ型楕円曲線への変換パラメタsの値を小さくすることにより、ステップ1813乃至はステップ1816における乗算の計算量を削減することができる。

次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力するアルゴリズムについて説明する。

第10実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、第9実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及び

- ワイエルシュトラス型楕円曲線上の点Pから、 X_d , Z_d , X_{d+1} , Z_{d+1} を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部202において上記アルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、 X_d , Z_d , X_{d+1} , Z_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- スカラー倍計算部103における座標復元部203の座標復元に必要な計算量は $15M + 2S$ であり、これは高速スカラー倍計算部202の高速スカラー倍計算に必要な計算量の $(9.2k - 3.6)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 13)M$ と見積もることができる。例えばスカラー値dが160ビット($k = 160$)であれば、このスカラー倍計算に必要な計算量は1485Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要な計算量はおよそ1600Mであり、これと比べて必要となる計算量は削減されている。

- 第11実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部103が、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部103に入力すると高速スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部202は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点

- (d-1)P=($X_{d-1}, Y_{d-1}, Z_{d-1}$)の座標のうち X_{d-1} 及び Z_{d-1} を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たにP=(x, y)とおく。高速スカラー倍計算部202は、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}, x$ 及びyを座標復元部203に与える。座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}, x$ 及びyよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP=(x_d, y_d)の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部103はワイエルシュトラス型楕円曲線上でアフィン座標において完全に座標が与えられたス
- 10 スカラー倍点(x_d, y_d)を計算結果として出力する。

次に図19により、座標x, y, $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ が与えられた場合に x_d, y_d を出力する座標復元部の処理について説明する。

- 座標復元部203では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP=(X_d, Y_d, Z_d)の座標うち X_d 及び Z_d 、射影座標で表されたモンゴ
- 15 メリ型楕円曲線上の点(d+1)P=($X_{d+1}, Y_{d+1}, Z_{d+1}$)の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点(d-1)P=($X_{d-1}, Y_{d-1}, Z_{d-1}$)の座標のうち X_{d-1} 及び Z_{d-1} 、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でワイエルシュトラス型楕円曲線上でアフィン座標において完全な座標が
- 20 与えられたスカラー倍点(x_d, y_d)を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を(X_1, Y_1, Z_1)でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を(x_d^{Mon}, y_d^{Mon})で、射影座標を(X_d, Y_d, Z_d)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d-1)Pのアフィン座標を(x_{d-1}, y_{d-1})で、射影座標を($X_{d-1}, Y_{d-1}, Z_{d-1}$)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を(x_{d+1}, y_{d+1})で、射影座標を($X_{d+1}, Y_{d+1}, Z_{d+1}$)でそれぞれ表す。
- 25

ステップ1901において $X_{d-1} \times Z_{d+1}$ が計算され、レジスタ T_1 に格納される。ステップ1902において $Z_{d-1} \times X_{d+1}$ が計算され、レジスタ T_2 に格

- 納される。ステップ1903において $T_1 - T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1}Z_{d+1}$ がレジスタ T_2 には $Z_{d-1}X_{d+1}$ がそれぞれ格納されており、したがって $X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ1904において $Z_d \times X$ が計算され、レジスタ T_2
- 5 に格納される。ステップ1905において $X_d - T_2$ が計算される。ここでレジスタ T_2 には $Z_d X$ が格納されており、したがって $X_d - xZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1906において T_2 の2乗が計算される。ここでレジスタ T_2 には $X_d - xZ_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1907において
- 10 $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1}$ がレジスタ T_2 には $(X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $(X_d - xZ_d)^2 (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ が計算される。その結果がレジスタ T_1 に格納される。ステップ1908において $4B \times y$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1909において $T_2 \times Z_{d+1}$ が計算される。ここでレ
- 15 ジスタ T_2 には $4By$ が格納されており、したがって $4ByZ_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1910において $T_2 \times Z_{d-1}$ が計算される。ここでレジスタ T_2 には $4ByZ_{d+1}$ が格納されており、したがって $4ByZ_{d-1}Z_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1911において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4ByZ_{d-1}$
- 20 Z_{d+1} が格納されており、したがって $4ByZ_{d-1}Z_{d+1}Z_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1912において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $4ByZ_{d-1}Z_{d+1}Z_d$ が格納されており、したがって $4ByZ_{d-1}Z_{d+1}Z_dX_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ1913において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には
- 25 $4ByZ_{d-1}Z_{d+1}Z_d$ が格納されており、したがって $4ByZ_{d-1}Z_{d+1}Z_dZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1914において、 $T_2 \times s$ が計算される。ここでレジスタ T_2 には $4ByZ_{d-1}Z_{d+1}Z_dZ_d$ が格納されており、したがって $4sByZ_{d-1}Z_{d+1}Z_dZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ1915においてレジスタ T_2 の逆元が計算される。

- ここでレジスタ T_2 には $4sByZ_{d-1}Z_{d+1}Z_dZ_d$ が格納されており、したがって $1/4sByZ_{d-1}Z_{d+1}Z_dZ_d$ が計算される。その結果がレジスタ T_2 に格納される。
- ステップ 1 4 1 6 において $T_2 \times T_3$ が計算される。ここでレジスタ T_2 には $1/4sByZ_{d-1}Z_{d+1}Z_dZ_d$ がレジスタ T_3 には $4ByZ_{d-1}Z_{d+1}Z_dX_d$ がそれぞれ格納されており、したがって $(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d)$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 1 9 1 7 において $T_3 + \alpha$ が計算される。ここでレジスタ T_3 には $(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d)$ が格納されており、したがって $(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d) + \alpha$ が計算される。その結果がレジスタ x_d に格納される。ステップ 1 9 1 8 においてレジスタ $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(X_d - xZ_d)^2 (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ がレジスタ T_2 には $1/4sByZ_{d-1}Z_{d+1}Z_dZ_d$ がそれぞれ格納されており、したがって $(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_dx)^2/4sByZ_{d-1}Z_{d+1}Z_d^2$ が計算される。その結果がレジスタ y_d に格納される。したがってレジスタ y_d には $(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_dx)^2/4sByZ_{d-1}Z_{d+1}Z_d^2$ が格納されている。レジスタ x_d にはステップ 1 9 1 7 において $(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d) + \alpha$ が格納され、その後更新が行なわれないので、その値が保持されている。

- 上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 X_{d-1} 、 Z_{d-1} からワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 3 8、数 3 9 を得る。両辺を各々減算することにより、数 4 0 を得る。したがって、数 4 1 となる。ここで $x_d^{Mon} = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ 、 $x_{d-1} = X_{d-1}/Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、数 4 2 を得る。 $x_d^{Mon} = X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d^{Mon} の分母と通分することにより、数 5 3 となる。

$$x_d^{Mon} = (4ByZ_{d+1}Z_{d-1}Z_dX_d)/(4ByZ_{d+1}Z_{d-1}Z_dZ_d) \cdots \text{数 5 3}$$

モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応

関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタを s, α として、 $y_d = s^{-1} y_d^{\text{Mon}}$ 及び $x_d = s^{-1} x_d^{\text{Mon}} + \alpha$ の関係がある。結果として次の式を得る。

$$y_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2 / 4sByZ_{d-1}Z_{d+1}Z_d^2 \cdots \text{数 } 5 \ 4$$

$$x_d = (4ByZ_{d+1}Z_{d-1}Z_dX_d) / (4sByZ_{d+1}Z_{d-1}Z_dZ_d) + \alpha \cdots \text{数 } 5 \ 5$$

ここで、 x_d, y_d は図 19 により与えられる。したがって、ワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における値が全て復元されることになる。

上記手順はステップ 1901、ステップ 1902、ステップ 1904、ステップ 1907、ステップ 1908、ステップ 1909、ステップ 1910、ステップ 1911、ステップ 1912、ステップ 1913、ステップ 1914、ステップ 1916 及びステップ 1918 において有限体上の乗算の計算量を必要とする。また、ステップ 1906 において有限体上の 2 乗算の計算量を必要とする。また、ステップ 1914 において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S 及び有限体上の逆元演算の計算量を I とすると、上記手順は $13M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 160 ビットであれば、高速スカラー倍計算の計算量はおおよそ $1500M$ 弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は $53.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた x_d, y_d の値が計算できれば x_d, y_d の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタである B の値乃至はモンゴメリ型楕円曲線への変換パラメタである s の値を小さくすること

により、ステップ1908乃至はステップ1914における乗算の計算量を削減することができる。

次に図10により、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部202では、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P を入力し、以下の手順によりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P=(X_{d-1}, Y_{d-1}, Z_{d-1})$ のうち X_{d-1} 及び Z_{d-1} を出力する。ステップ1016として、与えられたワイエルシュトラス型楕円曲線上の点 P をモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点 P とする。ステップ1001として、変数 I に初期値1を代入する。ステップ1002として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点 $2P$ を計算する。ステップ1003として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ1002で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ1004として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すればステップ $m=d$ となり、1014へ行く。一致しなければステップ1005へ行く。ステップ1005として、変数 I を1増加させる。ステップ1006として、スカラー値の I 番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ1007へ行く。そのビットの値が1であればステップ1010へ行く。ステップ1007として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ1008へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ1008として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍

- 算 2 (mP)を行ない、点2mPを計算する。その後ステップ1 0 0 9へ行く。ここで、
2 倍算2 (mP)は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用い
て計算される。ステップ1 0 0 9として、ステップ1 0 0 8で求めた点2mPとス
テップ1 0 0 7で求めた点(2m+1)Pを点の組(2mP, (2m+1)P)として、点の組(mP,
5 (m+1)P)の代わりに格納する。その後ステップ1 0 0 4へ戻る。ここで、点 2 mP、
点(2m+1)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステッ
プ1 0 1 0として、射影座標により表された点の組(mP, (m+1)P)から点mPと点
(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ1
0 1 1へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標に
10 おける加算公式を用いて計算される。ステップ1 0 1 1として、射影座標により
表された点の組(mP, (m+1)P)から点(m+1)Pの 2 倍算2((m+1)P)を行ない、点
(2m+2)Pを計算する。その後ステップ1 0 1 2へ行く。ここで、2 倍算2((m+
1)P)は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算
される。ステップ1 0 1 2として、ステップ1 0 1 0で求めた点(2m+1)Pとステ
15 ュップ1 0 1 1で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP,
(m+1)P)の代わりに格納する。その後ステップ1 0 0 4へ戻る。ここで、点
(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。
ステップ1 0 1 4として、射影座標で表された点の組(mP, (m+1)P)から、点(m-
1)Pの射影座標におけるX座標 X_{m-1} 及びZ座標を Z_{m-1} 求め、それぞれ X_{d-1} 及
20 び Z_{d-1} とする。その後ステップ1 0 1 3へ行く。ステップ1 0 1 3として、射
影座標で表された点mP=(X_m, Y_m, Z_m)より X_m 及び Z_m をそれぞれ X_d 及び Z_d とし
て、射影座標で表された点(m+1)P=($X_{m+1}, Y_{m+1}, Z_{m+1}$)より X_{m+1} 及び
 Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} として、 X_{d-1} 及び Z_{d-1} と共に出力する。
ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式
25 及び2 倍算の公式ではY座標を求める事ができないので、求まっていない。また
上記手順により、mとスカラー値dはビット長が等しくさらにそのビットのパタ
ーンも同じとなる為、等しくなる。

また、ステップ1 0 1 4において(m-1)Pを求める際に、数1 3、数1 4の公式
より求めてもよいし、mが奇数であれば、((m-1)/2)Pの値をステップ1 0 1 2の

段階で別に保持しておき、その値からモンゴメリ型楕円曲線の2倍の公式より、 $(m-1)P$ を求めてもよい。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ とすることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M+2S$ である。スカラー値の i 番目のビットの値が0であれば、ステップ1007において加算の計算量、ステップ1008において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の i 番目のビットの値が1であれば、ステップ1010において加算の計算量、
- 10 ステップ1011において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要である。いずれの場合においても $6M+4S$ の計算量が必要である。ステップ1004、ステップ1005、ステップ1006、ステップ1007、ステップ1008、ステップ1009乃至はステップ1004、ステップ1005、ステップ1006、ステップ1010、ステップ1011、ステップ1012の繰り返しの回数は、(スカラー値 d のビット長) -1 回となるので、
- 15 ステップ1002での2倍算の計算量とステップ1014での $(m-1)P$ の計算に必要な計算量を考慮に入れると、全体の計算量は $(6M+4S)k+M$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S=0.8M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k+3)M$ となる。例えばスカラー値 d が160ビット ($k=160$) であれば、上記手順のアルゴリズムの計算量はおおよそ1475Mとなる。スカラー値 d のビットあたりの計算量としてはおおよそ9.2Mとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、
- 25 ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ10Mと見積もられる。例えばスカラー値 d が160ビット ($k=160$) であれば、このスカラー倍計算方法の計算量はおおよそ1600Mと

なる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

- 尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 X_d , Y_d , X_{d+1} , Z_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $13M + S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 1)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M$ 、 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 56.8)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量はおよそ 1529M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおよそ 1640M であり、これと比べて必要となる計算量は削減されている。

- 第 12 実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いる。スカラー倍計算部 103 がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点 (X_d^W, Y_d^W, Z_d^W) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点

$(d-1)P=(X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} を計算し、射影座標で表された入力されたワイエルシュトラス型楕円曲線上の点 $P=(x, y)$ と共にその情報を座標復元部 203 に与える。座標変換部 203 は与えられた座標の値

- $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}, x$ 及び y よりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d^W, Y_d^W, Z_d^W)$ の座標 X_d^W, Y_d^W 及び Z_d^W の復元を行なう。スカラー倍計算部 103 はワイエルシュトラス型楕円曲線上で座標射影座標において完全に座標が与えられたスカラー倍点 (X_d^W, Y_d^W, Z_d^W) を計算結果として出力する。

- 次に図 20 により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ が与えられた場合に X_d^W, Y_d^W, Z_d^W を出力する座標復元部の処理について説明する。

- 座標復元部 203 では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P=(X_{d-1}, Y_{d-1}, Z_{d-1})$ の座標のうち X_{d-1} 及び Z_{d-1} 、スカラー倍計算部 103 に入力されたワイエルシュトラス型楕円曲線上の点 P を射影座標で表した (x, y) を入力し、以下の手順でワイエルシュトラス型楕円曲線上で射影座標において完全な座標が与えられたスカラー倍点 (X_d^W, Y_d^W, Z_d^W) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d-1)P$ のアフィン座標を (x_{d-1}, y_{d-1}) で、射影座標を $(X_{d-1}, Y_{d-1}, Z_{d-1})$ でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

ステップ 2001 において $X_{d-1} \times Z_{d+1}$ が計算され、レジスタ T_1 に格納される。ステップ 2002 において $Z_{d-1} \times X_{d+1}$ が計算され、レジスタ T_2 に格納される。ステップ 2003 において $T_1 - T_2$ が計算される。ここでレジスタ

- T_1 には $X_{d-1}Z_{d+1}$ がレジスタ T_2 には $Z_{d-1}X_{d+1}$ がそれぞれ格納されており、したがって $X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ2004において $Z_d \times x$ が計算され、レジスタ T_2 に格納される。ステップ2005において X_d-T_2 が計算される。ここでレジスタ
- 5 T_2 には $Z_d x$ が格納されており、したがって X_d-xZ_d が計算される。その結果がレジスタ T_2 に格納される。ステップ2006において T_2 の2乗が計算される。ここでレジスタ T_2 には X_d-xZ_d が格納されており、したがって $(X_d-xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ2007において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$ が
- 10 レジスタ T_2 には $(X_d-xZ_d)^2$ がそれぞれ格納されており、したがって $(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$ が計算される。その結果が Y_d^W に格納される。ステップ2008において $4B \times y$ が計算される。その結果がレジスタ T_2 に格納される。ステップ2009において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $4By$ が格納されており、したがって $4ByZ_{d+1}$ が計算される。その結
- 15 果がレジスタ T_2 に格納される。ステップ2010において $T_2 \times Z_{d-1}$ が計算される。ここでレジスタ T_2 には $4ByZ_{d+1}$ が格納されており、したがって $4ByZ_{d+1}Z_{d-1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ2011において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4yZ_{d+1}Z_{d-1}$ が格納されており、したがって $4ByZ_{d+1}Z_{d-1}Z_d$ が計算される。その結
- 20 果がレジスタ T_2 に格納される。ステップ2012において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $4ByZ_{d+1}Z_{d-1}Z_d$ が格納されており、したがって $4ByZ_{d+1}Z_{d-1}Z_dX_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ2013において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $4ByZ_{d+1}Z_{d-1}Z_d$ が格納されており、したがって $4ByZ_{d+1}Z_{d-1}Z_dZ_d$ が計算
- 25 される。その結果がレジスタ T_2 に格納される。ステップ2014において $T_2 \times s$ が計算される。ここでレジスタ T_2 には $4ByZ_{d+1}Z_{d-1}Z_dZ_d$ が格納されており、したがって $4sByZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果がレジスタ Z_d^W に格納される。ステップ2015において $\alpha \times Z_d^W$ が計算される。ここでレジスタ Z_d^W には $4sByZ_{d+1}Z_{d-1}Z_dZ_d$ が格納されており、したがって

- 4 $\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果がレジスタ T_2 に格納される。
- ステップ 2016 において $T_1 + T_2$ が計算される。ここでレジスタ T_1 には $4ByZ_{d+1}Z_{d-1}Z_dX_d$ がレジスタ T_2 には $4\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$ がそれぞれ格納されており、したがって $4ByZ_{d+1}Z_{d-1}Z_dX_d + 4\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$ が計算される。その結果がレジスタ X_d^W に格納される。したがってレジスタ X_d^W には $4ByZ_{d+1}Z_{d-1}Z_dX_d + 4\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$ が格納されている。レジスタ Y_d^W にはステップ 2007 において $(X_d - xZ_d)^2 (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$ が格納され、その後更新が行なわれないので、その値が保持されている。レジスタ Z_d^W にはステップ 2014 において $4sByZ_{d+1}Z_{d-1}Z_dZ_d$ が格納され、その後更新が行なわれないので、その値が保持されている。

- 上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} 、 X_{d-1} 、 Z_{d-1} からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標 (X_d^W, Y_d^W, Z_d^W) における値が全て復元される理由は以下の通りである。尚、点 $(d+1)P$ は点 dP に点 P を加算した点であり、点 $(d-1)P$ は点 dP から点 P を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 6、数 7 を得る。両辺を各々減算することにより、数 8 を得る。したがって、数 9 となる。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ 、 $x_{d-1} = X_{d-1}/Z_{d-1}$ であり、この値を代入することにより射影座標の値へと変換すると、数 10 を得る。

- 20 $x_d = X_d/Z_d$ であるが、 y_d の分母と通分することにより、数 20 となる。その結果として、

$$Y'_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_dx)^2 \cdots \text{数 5 6}$$

とし、

$$X'_d = 4ByZ_{d+1}Z_{d-1}Z_dX_d \cdots \text{数 5 7}$$

- 25 $Z'_d = 4ByZ_{d+1}Z_{d-1}Z_dZ_d \cdots \text{数 5 8}$

とすると $(X'_d, Y'_d, Z'_d) = (X_d, X_d, X_d)$ となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751

(2000) pp. 238-257 に記載されている。それによると、変換パラメタを s, α として、 $Y_d^W = Y'_d$ 、 $X_d^W = X'_d + \alpha Z_d^W$ 及び $Z_d^W = sZ'_d$ の関係がある。結果として次の式を得る。

$$Y_d^W = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2 \cdots \text{数 } 5 \ 9$$

$$5 \quad X_d^W = 4ByZ_{d+1}Z_{d-1}Z_dX_d + \alpha 4sByZ_{d+1}Z_{d-1}Z_dZ_d \cdots \text{数 } 6 \ 0$$

$$Z_d^W = 4sByZ_{d+1}Z_{d-1}Z_dZ_d \cdots \text{数 } 6 \ 1$$

となる。ここで、 X_d^W 、 Y_d^W 、 Z_d^W は図 20 により与えられる。したがって、ワイエルシュトラス型楕円曲線における射影座標 (X_d^W, Y_d^W, Z_d^W) の値が全て復元されていることになる。

- 10 上記手順はステップ 2001、ステップ 2002、ステップ 2004、ステップ 2007、ステップ 2008、ステップ 2009、ステップ 2010、ステップ 2011、ステップ 2012、ステップ 2013、ステップ 2014 及びステップ 2015 において有限体上の乗算の計算量を必要とする。また、ステップ 2006 において有限体上の 2 乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S とすると、上記手順は $12M + S$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 160 ビットであれば、高速スカラー倍計算の計算量はおおよそ $1500M$ 弱と見積もられる。
- 15
- 20 $S = 0.8M$ と仮定すると座標復元の計算量は $12.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

- 尚、上記手順をとらなくても、上記計算式により与えられた X_d^W 、 Y_d^W 、 Z_d^W の値が計算できれば X_d^W 、 Y_d^W 、 Z_d^W の値が復元できる。また、ワイエルシュトラス型楕円曲線においてアフィン座標におけるスカラー倍点 dP を $dP = (x_d^W, y_d^W)$ とすると、 x_d^W 、 y_d^W が上記計算式により与えられる値を取るように X_d^W 、 Y_d^W 、 Z_d^W の値を選択し、その値が計算できれば X_d^W 、 Y_d^W 、 Z_d^W が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタである B やモンゴメリ型楕円曲線への変換パラ
- 25

メタである s の値を小さくすることにより、ステップ 2008 乃至はステップ 2014 における乗算の計算量を削減することができる。

次に、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムについて説明する。

- 5 第12実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、第11実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部202において上記手順のアルゴリズムを用
- 10 いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- スカラー倍計算部103における座標復元部203の座標復元に必要な計算量は $12M + S$ であり、これは高速スカラー倍計算部202の高速スカラー倍計算
- 15 に必要な計算量の $(9.2k + 1)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 13.8)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー
- 20 倍計算に必要な計算量はおよそ $1486M$ となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要な計算量はおよそ $1600M$ であり、これと比べて必要となる計算量は削減されている。

- 25 第13実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部103が、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点

- (x_d^W, y_d^W) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部 1 0 3に入力すると高速スカラー倍計算部 2 0 2 がそれを受け取る。高速スカラー倍計算部 2 0 2 は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ の座標のうち x_{d-1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 2 0 3 に与える。座標復元部 2 0 3 は与えられた座標の値 x_d, x_{d+1}, x_{d-1}, x 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d^W, y_d^W)$ の座標 y_d^W の復元を行なう。スカラー倍計算部 1 0 3 はワイエルシュトラス型楕円曲線上でアフィン座標において完全に座標が与えられたスカラー倍点 (x_d^W, y_d^W) を計算結果として出力する。
- 次に図 2 1 により、座標 $x, y, x_d, x_{d+1}, x_{d-1}$ が与えられた場合に、 x_d^W, y_d^W を出力する座標復元部の処理について説明する。

- 座標復元部 2 0 3 では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ の座標のうち x_{d-1} 、スカラー倍計算部 1 0 3 に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d^W, y_d^W) を出力する。

- ステップ 2 1 0 1 において $x_d - x$ が計算され、レジスタ T_1 に格納される。ステップ 2 1 0 2 において T_1 の 2 乗すなわち $(x_d - x)^2$ が計算され、レジスタ T_1 に格納される。ステップ 2 1 0 3 において $x_{d-1} - x_{d+1}$ が計算され、レジスタ T_2 に格納される。ステップ 2 1 0 4 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(x_d - x)^2$ がレジスタ T_2 には $x_{d-1} - x_{d+1}$ がそれぞれ格納されており、したがって $(x_d - x)^2 (x_{d-1} - x_{d+1})$ が計算される。その結果

- がレジスタ T_1 に格納される。ステップ 2105 において $4B \times y$ が計算され、レジスタ T_2 に格納される。ステップ 2106 において T_2 の逆元が計算される。ここでレジスタ T_2 には $4By$ が格納されており、したがって $1/4By$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 2107 において $T_1 \times T_2$ が
- 5 計算される。ここでレジスタ T_1 には $(x_d - x)^2 (x_{d-1} - x_{d+1})$ がレジスタ T_2 には $1/4By$ がそれぞれ格納されており、したがって $(x_d - x)^2 (x_{d-1} - x_{d+1})/4By$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 2108 において $T_1 \times s^{-1}$ が計算される。ここでレジスタ T_1 には $(x_d - x)^2 (x_{d-1} - x_{d+1})/4sBy$ が格納されており、したがって $(x_d - x)^2 (x_{d-1} - x_{d+1})/4sBy$ が計算される。その結果がレジスタ y_d^W に格納される。尚、 s はあらかじめ与えられている値であり、したがってあらかじめ s^{-1} を計算できる。ステップ 2109 において $x_d \times s^{-1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 2110 において $T_1 + \alpha$ が計算される。ここでレジスタ T_1 には $s^{-1} x_d$ が格納されており、したがって $s^{-1} x_d + \alpha$ が計算される。その
- 15 結果がレジスタ x_d^W に格納される。したがってレジスタ x_d^W には $s^{-1} x_d + \alpha$ が格納されている。レジスタ y_d^W はステップ 2108 において $(x_d - x)^2 (x_{d-1} - x_{d+1})/4sBy$ が格納され、その後更新されないで、その値が保持されている。
- 上記手順によりスカラー倍点の y 座標 y_d が復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。点 $(d-1)P$ は点 dP から点 P を減算した点
- 20 である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 6、数 7 を得る。両辺を各々減算することにより、数 8 を得る。したがって、数 9 となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications,
- 25 Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタを s, α として、 $y_d^W = s^{-1} y_d$ 及び $x_d^W = s^{-1} x_d + \alpha$ の関係がある。結果として次の式を得る。

$$y_d^W = (x_{d-1} - x_{d+1})(x_d - x)^2 / 4sBy \quad \cdots \text{数 6 2}$$

$$x_d^W = s^{-1} x_d + \alpha \quad \cdots \text{数 6 3}$$

ここで、 x_d^W 、 y_d^W は図21により与えられる。したがって、アフィン座標 (x_d^W, y_d^W) の値は全て復元されていることになる。

上記手順はステップ2104、ステップ2105、ステップ2107、ステップ2108及びステップ2109において有限体上の乗算の計算量を必要とする。

- 5 また、ステップ2102において有限体上の2乗算の計算量を必要とする。さらにステップ2106において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の2乗算の計算量をS、有限体上の逆元演算の計算量をIとすると、上記手順は $5M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500M弱と見積もられる。S = 0.8M及びI = 40Mと仮定すると座標復元の計算量は45.8Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を
- 15 復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば y_d^W の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBやモンゴメリ型楕円曲線への変換パラメタsの値を小さくすることにより、ステップ2105、ステップ2108乃至はステップ2109における乗算の計算量を削減することができる。

20

次に図24により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、 x_d 、 x_{d+1} 、 x_{d-1} を出力する高速スカラー倍計算部の処理について説明する。

- 高速スカラー倍計算部202では、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP=(x_d, y_d)$ のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(x_{d+1}, y_{d+1})$ のうち x_{d+1} 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d-1)P=(x_{d-1}, y_{d-1})$ のうち x_{d-1} を出力する。ステップ2416として、与えられ
- 25

- たワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ2401として、変数Iに初期値1を代入する。ステップ2402として、点Pの2倍点2Pを計算する。ここで点Pは射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点2Pを計算する。ステップ2403として、スカラー倍計算部103に入力された楕円曲線上の点Pとステップ2402で求めた点2Pを、点の組 $(P, 2P)$ として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ2404として、変数Iとスカラー値dのビット長とが一致するかどうかを判定し、一致すれば $m = d$ となり、ステップ2414へ行く。一致しなければステップ2405へ行く。ステップ2405として、変数Iを1増加させる。ステップ2406として、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ2407へ行く。そのビットの値が1であればステップ2410へ行く。ステップ2407として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2408へ行く。ここで、加算 $mP + (m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ2408として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ2409へ行く。ここで、2倍算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ2409として、ステップ2408で求めた点 $2mP$ とステップ2407で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ2404へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ2410として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP + (m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ2411へ行く。ここで、加算 $mP + (m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ2411として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステ

- ステップ 2 4 1 2 へ行く。ここで、2 倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算される。ステップ 2 4 1 2 として、ステップ 2 4 1 0 で求めた点 $(2m+1)P$ とステップ 2 4 1 1 で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 2 4 0 4 へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ 2 4 1 4 として、射影座標で表された点の組 $(mP, (m+1)P)$ から、点 $(m-1)P$ の射影座標における X 座標 X_{m-1} 及び Z 座標 Z_{m-1} を求め、それぞれ X_{d-1} 及び Z_{d-1} とする。その後ステップ 2 4 1 5 へ行く。ステップ 2 4 1 5 として、射影座標で表された点 $mP = (X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d とし、射影座標で表された点 $(m+1)P = (X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} とする。ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び 2 倍算の公式では Y 座標を求める事ができないので、求まっていない。 $X_{d-1}, Z_{d+1}, X_d, Z_d, X_{d+1}, Z_{d+1}$ より、数 2 4、数 2 5、数 2 6 として x_{d-1}, x_d, x_{d+1} を求める。その後ステップ 2 4 1 3 へ行く。ステップ 2 4 1 3 として、 x_{d-1}, x_d, x_{d+1} を出力する。上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ 2 4 1 4 において $(m-1)P$ を求める際に、数 1 3、数 1 4 の公式により求めてもよいし、 m が奇数であれば、 $((m-1)/2)P$ の値をステップ 2 4 1 2 の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の 2 倍算の公式より、 $(m-1)P$ を求めてもよい。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ とすることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の 2 乗算の計算量である。モンゴメリ型楕円曲線の射影座標における 2 倍算の公式の計算量は、 $3M+2S$ である。スカラー値の I 番目のビットの値が 0 であれば、ステップ 2 4 0 7 において加算の計算量、ステップ 2 4 0 8 において 2 倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が 1 であれば、ステップ 2 4 1 0 において加算の計算量、ステップ 2 4 1 1 において 2 倍算の計算量が必要となる。すなわち $6M+4S$ の

- 計算量が必要である。いずれの場合においても $6M + 4S$ の計算量が必要である。
- ステップ 2404、ステップ 2405、ステップ 2406、ステップ 2407、ステップ 2408、ステップ 2409 乃至はステップ 2404、ステップ 2405、ステップ 2406、ステップ 2410、ステップ 2411、ステップ 2412 の繰り返しの回数は、(スカラー値 d のビット長) -1 回となるので、ステップ 2402 での 2 倍算の計算量、ステップ 2414 での $(m-1)P$ の計算に必要な計算量及びステップ 2415 でのアフィン座標への変換の計算量を考慮に入れると、全体の計算量は $(6M + 4S)k + 11M + I$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S = 0.8M$ 程度、計算量 I は $I = 40M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k + 51)M$ となる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、上記手順のアルゴリズムの計算量はおおよそ 1523M となる。スカラー値 d のビットあたりの計算量としてはおおよそ $9.2M$ となる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates,
- 15 Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ 10M と見積もられ、これ以外にアフィン座標
- 20 への変換の計算量が必要となる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算方法の計算量はおおよそ 1640M となる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。
- 尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 x_{d-1} ,
- 25 x_d , x_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

第 14 の実施例は、スカラー倍計算部 103 がスカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものであ

- る。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部 1 0 3 に入力すると高速スカラー倍計算部 2 0 2 がそれを受け取る。高速スカラー倍計算部 2 0 2 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 2 0 3 に与える。座標復元部 2 0 3 は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部 1 0 3 はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。

次に図 3 4 により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に x_d, y_d を出力する座標復元部の処理について説明する。

- 座標復元部 2 0 3 では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標うち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部 1 0 3 に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

ステップ 3 4 0 1 において $x \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ 3 4 0 2 において $X_d + T_1$ が計算される。ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d + X_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 3 4 0 3 において $X_d - T_1$ が計算され、ここでレジスタ

- T_1 には xZ_d が格納されており、したがって $xZ_d - X_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3404においてレジスタ T_3 の2乗が計算される。ここでレジスタ T_3 には $xZ_d - X_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3405
- 5 において $T_3 \times X_{d+1}$ が計算される。ここでレジスタ T_3 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3406において $2A \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ3407において $T_2 + T_1$ が計算される。ここでレジスタ T_2 には $xZ_d + X_d$ がレジスタ T_1 には $2AZ_d$ がそれぞれ格納されており、したがって $xZ_d + X_d + 2AZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3408において $x \times X_d$ が計算され、レジスタ T_4 に格納される。ステップ3409において $T_4 + Z_d$ が計算される。ここでレジスタ T_4 には xX_d が格納されており、したがって $xX_d + Z_d$ が計算される。その結果がレジスタ T_4 に格納される。ステップ3410において $T_2 \times T_4$ が計算される。ここでレジスタ
- 15 T_2 には $xZ_d + X_d + 2AZ_d$ がレジスタ T_4 には $xX_d + Z_d$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3411において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2AZ_d$ が格納されており、したがって $2AZ_d^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3412において $T_2 - T_1$ が計算される。
- 20 ここでレジスタ T_2 には $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ がここでレジスタ T_1 には $2AZ_d^2$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3413において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2$ が格納されており、したがって $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ が計算される。その結果がレジスタ T_2 に格納される。
- 25 ステップ3414において $T_2 - T_3$ が計算される。ここでレジスタ T_2 には $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ がレジスタ T_3 には $X_{d+1}(X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納され

- る。ステップ 3 4 1 5 において $2B \times y$ が計算され、レジスタ T_1 に格納される。
- ステップ 3 4 1 6 において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2By$ が格納されており、したがって $2ByZ_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 3 4 1 7 において $T_1 \times Z_{d+1}$ が計算される。ここでレジスタ T_1 には $2ByZ_d$ が格納されており、したがって $2ByZ_d Z_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 3 4 1 8 において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1}$ が格納されており、したがって $2ByZ_d Z_{d+1} Z_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 3 4 1 9 においてレジスタ T_3 の逆元が計算される。ここでレジスタ T_3 には $2ByZ_d Z_{d+1} Z_d$ が格納されており、したがって $1/2ByZ_d Z_{d+1} Z_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 3 4 2 0 において $T_2 \times T_3$ が計算される。ここでレジスタ T_2 には $Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1} (X_d - xZ_d)^2$ がレジスタ T_3 には $1/2ByZ_d Z_{d+1} Z_d$ がそれぞれ格納されており、したがって $\{Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1} (X_d - xZ_d)^2\} / 2ByZ_d Z_{d+1} Z_d$ が計算される。その結果がレジスタ y_d に格納される。ステップ 3 4 2 1 において $T_1 \times X_d$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1}$ が格納されており、したがって $2ByZ_d Z_{d+1} X_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 3 4 2 2 において $T_1 \times T_3$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1} X_d$ がレジスタ T_3 には $1/2ByZ_d Z_{d+1} Z_d$ がそれぞれ格納されており、したがって $2ByZ_d Z_{d+1} X_d / 2ByZ_d Z_{d+1} Z_d (= X_d / Z_d)$ が計算される。その結果が x_d に格納される。 y_d にはステップ 3 4 2 0 において $\{Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1} (X_d - xZ_d)^2\} / 2ByZ_d Z_{d+1} Z_d$ が格納され、その後更新が行なわれないので、その値が保持されている。
- 25 上記手順により座標復元部 2 0 3 へ与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} からモンゴメリ型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における値が全て復元される理由は以下の通りである。尚、点 $(d+1)P$ は点 dP に点 P を加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 6 を得る。点 P 及び点 dP はモンゴメリ型楕円曲線上の点

であるので、 $By_d^2 = x_d^3 + Ax_d^2 + x_d$ 及び $By^2 = x^3 + Ax^2 + x$ をみたす。数6に代入し、 By_d^2 及び By^2 を消去し、式を整理すると、

$$y_d = \{(x_d x + 1)(x_d + x + 2A) - 2A - (x_d - x)^2 x_{d+1}\} / (2By) \quad \cdots \text{数6 4}$$

を得る。ここで $x_d = X_d / Z_d$ 、 $x_{d+1} = X_{d+1} / Z_{d+1}$ であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d = \{Z_{d+1} \{(X_d x + Z_d)(X_d + x Z_d + 2A Z_d) - 2A Z_d^2\} - (X_d - x Z_d)^2 X_{d+1}\} / (2B y Z_d Z_{d+1} Z_d) \quad \cdots \text{数6 5}$$

$x_d = X_d / Z_d$ であるが、逆元演算の回数を減らす目的で y_d の分母と通分することにより、

$$X_d = (2B y Z_d Z_{d+1} X_d) / (2B y Z_d Z_{d+1} Z_d) \quad \cdots \text{数6 6}$$

となる。ここで、 x_d 、 y_d は図34の処理により与えられている。したがって、アフィン座標 (x_d, y_d) の値が全て復元されていることになる。

上記手順はステップ3401、ステップ3405、ステップ3406、ステップ3408、ステップ3410、ステップ3411、ステップ3413、ステップ3415、ステップ3416、ステップ3417、ステップ3418、ステップ3420、ステップ3421及びステップ3422において有限体上の乗算の計算量を必要とする。また、ステップ3404において有限体上の2乗算の計算量を必要とする。また、ステップ3419において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、

2乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の2乗算の計算量を S 及び有限体上の逆元演算の計算量を I とすると、上記手順は $14M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が160ビットであれば、高速スカラー倍計算の計算量はおおよそ $1500M$ 弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は $54.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた x_d 、 y_d の値が計算できれば x_d 、 y_d の値が復元できる。その場合においては一般的に復元に

必要となる計算量が増大する。また、楕円曲線のパラメタであるA乃至はBの値を小さくすることにより、ステップ3406乃至はステップ3415における乗算の計算量を削減することができる。

次にスカラー値d及びモンゴメリ型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1},$

- 5 Z_{d+1} を出力する高速スカラー倍計算部の処理を説明する。

第14実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、第1実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算

10 部202において上記アルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- スカラー倍計算部103における座標復元部203の座標復元に必要な計算量は $14M + S + I$ であり、これは高速スカラー倍計算部202の高速スカラー倍
- 15 計算に必要な計算量の $(9.2k - 4.6)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M, S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 50)M$ と見積もることができる。例えばスカラー値dが160ビット ($k = 160$) であ
- 20 れば、このスカラー倍計算に必要な計算量は $1522M$ となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおおよそ $1640M$ であり、これと比べて必要となる計算量は削減されている。

- 25 第15の実施例は、スカラー倍計算部103がスカラー値d及びモンゴメリ型楕円曲線上の点Pから、モンゴメリ型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算し出力するものである。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部103に入力すると高速スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部20

- 2 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標 X_d, Y_d 及び Z_d の復元を行なう。スカラー倍計算部 103 は射影座標において完全に座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算結果として出力する。

次に図 35 により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に X_d, Y_d, Z_d を出力する座標復元部の処理について説明する。

- 座標復元部 203 では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部 103 に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順で射影座標において完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- ステップ 3501 において $x \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ 3502 において $X_d + T_1$ が計算される。ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d + X_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 3503 において $X_d - T_1$ が計算され、ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d - X_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 3504 においてレジスタ T_3 の 2 乗が計

- 算される。ここでレジスタ T_3 には $xZ_d - X_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 3505 において $T_3 \times X_{d+1}$ が計算される。ここでレジスタ T_3 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ
- 5 T_3 に格納される。ステップ 3506 において $2A \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ 3507 において $T_2 + T_1$ が計算される。ここでレジスタ T_2 には $xZ_d + X_d$ がレジスタ T_1 には $2AZ_d$ がそれぞれ格納されており、したがって $xZ_d + X_d + 2AZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 3508 において $x \times X_d$ が計算され、レジスタ T_4 に格納される。ステップ
- 10 3509 において $T_4 + Z_d$ が計算される。ここでレジスタ T_4 には xX_d が格納されており、したがって $xX_d + Z_d$ が計算される。その結果がレジスタ T_4 に格納される。ステップ 3510 において $T_2 \times T_4$ が計算される。ここでレジスタ T_2 には $xZ_d + X_d + 2AZ_d$ がレジスタ T_4 には $xX_d + Z_d$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ が計算される。その結果がレジスタ T_2 に
- 15 格納される。ステップ 3511 において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2AZ_d$ が格納されており、したがって $2AZ_d^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 3512 において $T_2 - T_1$ が計算される。ここでレジスタ T_2 には $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ がここでレジスタ T_1 には $2AZ_d^2$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d) -$
- 20 $2AZ_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 3513 において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2$ が格納されており、したがって $Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ が計算される。その結果がレジスタ T_2 に格納される。
- ステップ 3514 において $T_2 - T_3$ が計算される。ここでレジスタ T_2 には
- 25 $Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ がレジスタ T_3 には $X_{d+1} (X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ Y_d に格納される。ステップ 3515 において $2B \times y$ が計算され、レジスタ T_1 に格納される。ステップ 3516 において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2By$

が格納されており、したがって $2ByZ_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3517において $T_1 \times Z_{d+1}$ が計算される。ここでレジスタ T_1 には $2ByZ_d$ が格納されており、したがって $2ByZ_d Z_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3518において $T_1 \times X_d$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1}$ が格納されており、したがって $2ByZ_d Z_{d+1} X_d$ が計算される。その結果がレジスタ X_d に格納される。ステップ3519において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1}$ が格納されており、したがって $2ByZ_d Z_{d+1} Z_d$ が計算される。その結果がレジスタ Z_d に格納される。 X_d にはステップ3518において $2ByZ_d Z_{d+1} X_d$ が格納され、その後更新が行なわれないので、その値が保持されている。 Y_d にはステップ3514において $Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} からスカラー倍点の射影座標 (X_d, Y_d, Z_d) における値が全て復元される理由は以下の通りである。

点 $(d+1)P$ は点 dP に点 P を加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、次の数6を得る。点 P 及び点 dP はモンゴメリ型楕円曲線上の点であるので、 $By_d^2 = x_d^3 + Ax_d^2 + x_d$ 及び $By^2 = x^3 + Ax^2 + x$ をみだす。数6に代入し、 By_d^2 及び By^2 を消去し、式を整理すると、数64を得る。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ であり、この値を代入することにより射影座標の値へと変換すると、数65を得る。 $x_d = X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d の分母と通分することにより、数66となる。その結果として、

$$Y_d = Z_{d+1} [(X_d + xZ_d + 2AZ_d)(X_d x + Z_d) - 2AZ_d^2] - (X_d - xZ_d)^2 X_{d+1} \quad \dots \text{数67}$$

とし、 X_d 及び Z_d をそれぞれ

$$2ByZ_d Z_{d+1} X_d \quad \dots \text{数68}$$

$$2ByZ_d Z_{d+1} X_d \quad \dots \text{数69}$$

により更新すればよい。ここで、 X_d 、 Y_d 、 Z_d は図35の処理により与えられている。したがって、射影座標 (X_d, Y_d, Z_d) の値が全て復元されていることになる。

上記手順はステップ3501、ステップ3505、ステップ3506、ステッ

- プ 3 5 0 8、ステップ 3 5 1 0、ステップ 3 5 1 1、ステップ 3 5 1 3、ステップ 3 5 1 5、ステップ 3 5 1 6、ステップ 3 5 1 7、ステップ 3 5 1 8 及びステップ 3 5 1 9 において有限体上の乗算の計算量を必要とする。また、ステップ 3 5 0 4 において有限体上の 2 乗算の計算量を必要とする。有限体上の加算及び減
- 5 算の計算量は、有限体上の乗算の計算量、2 乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S とすると、上記手順は $12M + S$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 160 ビットであれば、高速スカラー倍計算の計算量はおおよそ $1500M$ 弱と見積もられる。
- 10 $S = 0.8M$ と仮定すると座標復元の計算量は $12.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた X_d 、 Y_d 、 Z_d の値が計算できれば X_d 、 Y_d 、 Z_d の値が復元できる。また、 x_d 、 y_d が上記計算式に

15 より与えられる値を取るように X_d 、 Y_d 、 Z_d の値を選択し、その値が計算できれば X_d 、 Y_d 、 Z_d が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタである A 乃至は B の値を小さくすることにより、ステップ 3 5 0 6 乃至はステップ 3 5 1 5 における乗算の計算量を削減することができる。

- 20 次に、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムについて説明する。

第 15 実施例の高速スカラー倍計算部 202 の高速スカラー倍計算方法として、第 1 実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴ

25 リズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部 202 において上記アルゴリズムを用いなくても、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量

は $12M + S$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k - 4.6)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 8)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量は 1480M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要な計算量はおおよそ 1600M であり、これと比べて必要となる計算量は削減されている。

第 16 の実施例は、スカラー倍計算部 103 がスカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力する。スカラー値 d 及びモンゴメリ型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたモンゴメリ型楕円曲線上の点 P からモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値 x_d 、 x_{d+1} 、 x 及び y よりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 y_d の復元を行なう。スカラー倍計算部 103 はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。

次に図 36 により、座標 x 、 y 、 x_d 、 x_{d+1} が与えられた場合に、 x_d 、 y_d を出力する座標復元部の処理について説明する。

座標復元部 203 では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴ

メリ型楕円曲線上の点 $(d+1)P=(x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。

- 5 ステップ3601において $x_d \times x$ が計算され、レジスタ T_1 に格納される。ステップ3602において T_1+1 が計算される。ここでレジスタ T_1 には $x_d x$ が格納されており、したがって $x_d x+1$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3603において x_d+x が計算され、レジスタ T_2 に格納される。ステップ3604において T_2+2A が計算される。ここでレジスタ T_2 には
- 10 x_d+x が格納されており、したがって x_d+x+2A が計算される。その結果がレジスタ T_2 に格納される。ステップ3605において $T_1 \times T_1$ が計算される。ここでレジスタ T_1 には $x_d x+1$ がレジスタ T_2 には x_d+x+2A がそれぞれ格納されており、したがって $(x_d x+1)(x_d+x+2A)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3606において T_1-2A が計算される。ここでレジスタ
- 15 T_1 には $(x_d x+1)(x_d+x+2A)$ が格納されており、したがって $(x_d x+1)(x_d+x+2A)-2A$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3607において x_d-x が計算され、レジスタ T_1 に格納される。ステップ3608において T_2 の2乗が計算される。ここでレジスタ T_2 には x_d-x が格納されており、したがって $(x_d-x)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ
- 20 3609において $T_2 \times x_{d+1}$ が計算される。ここでレジスタ T_2 には $(x_d-x)^2$ が格納されており、したがって $(x_d-x)^2 x_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3610において T_1-T_2 が計算される。ここでレジスタ T_1 には $(x_d x+1)(x_d+x+2A)-2A$ がレジスタ T_2 には $(x_d-x)^2$
- 25 x_{d+1} がそれぞれ格納されており、したがって $(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3611において $2B \times y$ が計算され、レジスタ T_2 に格納される。ステップ3612において T_2 の逆元が計算される。ここでレジスタ T_2 には $2By$ が格納されており、したがって $1/2By$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3613において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には

- $(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$ がレジスタ T_2 には $1/2By$ がそれぞれ格納されており、したがって $(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}/2By$ が計算される。その結果がレジスタ y_d に格納される。したがってレジスタ y_d には $(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}/2By$ が格納されている。レジスタ x_d は
- 5 全く更新されないので入力された値が保持されている。

- 上記手順によりスカラー倍点の y 座標 y_d が復元される理由は以下の通りである。尚、点 $(d+1)P$ は点 dP に点 P を加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数 6 を得る。点 P 及び点 dP はモンゴメリ型楕円曲線上の点であるので、 $By_d^2 = x_d^3 + Ax_d^2 + x_d$ 及び $By^2 = x^3 + Ax^2 + x$ をみたす。数 6 に代入し、 By_d^2 及び By^2 を消去し、式を整理すると、数 6 4 を得る。
- 10 ここで、 x_d, y_d は図 3 6 の処理により与えられる。したがって、アフィン座標 (x_d, y_d) の値は全て復元されたことになる。

- 上記手順はステップ 3 6 0 1、ステップ 3 6 0 5、ステップ 3 6 0 9、ステップ 3 6 1 1 及びステップ 3 6 1 3 において有限体上の乗算の計算量を必要とする。
- 15 また、ステップ 3 6 0 8 において有限体上の 2 乗算の計算量を必要とする。さらにステップ 3 6 1 2 において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S 、有限体上の逆元演算の計算量を I とすると、上
- 20 記手順は $5M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 1 6 0 ビットであれば、高速スカラー倍計算の計算量はおおよそ $1500M$ 弱と見積もられる。 $S = 0.8M$ 及び $I = 40M$ と仮定すると座標復元の計算量は $45.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元でき
- 25 ていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば y_d の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタである B の値を小さくすることにより、ステップ 2 6 0 5 における乗算の計算量を削減することができる。

次に図43により、スカラー値 d 及びモンゴメリ型楕円曲線上の点 P から、 x_d 、 x_{d+1} を出力する高速スカラー倍計算部の処理について説明する。

- 高速スカラー倍計算部202では、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点 P を入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP=(x_d, y_d)$ のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(x_{d+1}, y_{d+1})$ のうち x_{d+1} を出力する。ステップ4301として、変数 I に初期値1を代入する。ステップ4302として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点 $2P$ を計算する。ステップ4303として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ4302で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ4304として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すればステップ4315へ行く。一致しなければステップ4305へ行く。ステップ4305として、変数 I を1増加させる。ステップ4306として、スカラー値の I 番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ4307へ行く。そのビットの値が1であればステップ4310へ行く。ステップ4307として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ4308へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ4308として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ4309へ行く。ここで、2倍算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ4309として、ステップ4308で求めた点 $2mP$ とステップ4307で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ4304へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ4310として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点

- ($m+1$)Pの加算 $mP+(m+1)P$ を行ない、点($2m+1$)Pを計算する。その後ステップ4 3 1 1へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ4 3 1 1として、射影座標により表された点の組($mP, (m+1)P$)から点($m+1$)Pの2倍算 $2((m+1)P)$ を行ない、点
- 5 ($2m+2$)Pを計算する。その後ステップ4 3 1 2へ行く。ここで、2倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ4 3 1 2として、ステップ4 3 1 0で求めた点($2m+1$)Pとステップ4 3 1 1で求めた点($2m+2$)Pを点の組($(2m+1)P, (2m+2)P$)として、点の組($mP, (m+1)P$)の代わりに格納する。その後ステップ4 3 0 4へ戻る。ここで、点
- 10 ($2m+1$)P、点($2m+2$)P、点 mP 及び点($m+1$)Pは全て射影座標において表されている。ステップ4 3 1 5として、射影座標で表された点 $mP=(X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d とし、射影座標で表された点($m+1$)P= $(X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} とする。ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び
- 15 2倍算の公式ではY座標を求める事ができないので、求まっていない。 $X_d, Z_d, X_{d+1}, Z_{d+1}$ より、 $x_d=X_d Z_{d+1}/Z_d Z_{d+1}$, $x_{d+1}=Z_d X_{d+1}/Z_d Z_{d+1}$ として x_d, x_{d+1} を求める。その後ステップ4 3 1 3へ行く。ステップ4 3 1 3として、 x_d, x_{d+1} を出力する。上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。
- 20 モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ とすることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M+2S$ である。スカラー値の I 番目のビットの値が0であれば、ステップ4 3 0 7において加算の計算量、ステップ4 3 0 8において2倍
- 25 算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ4 3 1 0において加算の計算量、ステップ4 3 1 1において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要である。いずれの場合においても $6M+4S$ の計算量が必要である。ステップ4 3 0 4、ステップ4 3 0 5、ステップ4 3 0 6、ステップ4 3 0 7、

ステップ4308、ステップ4309乃至はステップ4304、ステップ4305、ステップ4306、ステップ4310、ステップ4311、ステップ4312の繰り返しの回数は、(スカラー値dのビット長) - 1回となるので、ステップ4302での2倍算の計算量及びアフィン座標への変換の計算量を考慮に入

5 ると、全体の計算量は $(6M + 4S)k + 2M - 2S + I$ となる。ここでkはスカラー値dのビット長である。一般的には、計算量Sは、 $S = 0.8M$ 程度、計算量Iは $I = 40M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k + 40.4)M$ となる。例えばスカラー値dが160ビット ($k = 160$)であれば、上記手順のアルゴリズムの計算量はおおよそ1512Mとなる。スカラー

10 値dのビットあたりの計算量としてはおおよそ9.2Mとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算

15 方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ10Mと見積もられ、これ以外にアフィン座標への変換の計算量が必要となる。例えばスカラー値dが160ビット ($k = 160$)であれば、このスカラー倍計算方法の計算量はおおよそ1640Mとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速と

20 いえる。

尚、高速スカラー倍計算部202において上記手順のアルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、 x_d 、 x_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部103における座標復元部203の座標復元に必要な計算量

25 は $5M + S + I$ であり、これは高速スカラー倍計算部202の高速スカラー倍計算に必要な計算量の $(9.2k + 40.4)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ 及び $I = 40M$ と仮定すると、この計算量はおおよそ $(9.2k + 86.$

- 2) Mと見積もることができる。例えばスカラー値 d が160ビット ($k=160$) であれば、このスカラー倍計算に必要な計算量はおよそ1558Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、
- 5 スカラー倍点をアフィン座標として出力する場合に必要な計算量はおよそ1640Mであり、これと比べて必要となる計算量は削減されている。

- 第17の実施例は、楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部103の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部103の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部103がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものである。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部103に入力すると高速スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部202は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点 $P=(x, y)$ と共にその情報を座標復元部203に与える。座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP=(x_d, y_d)$ の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部103はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。
- 25

次に図37により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に x_d, y_d を出力する座標復元部の処理について説明する。

座標復元部203では、ワイエルシュトラス型楕円曲線において射影座標で表

されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標うち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でア

- 5 フィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてワイエルシュトラス型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。ワイエルシュトラス型楕円曲
- 10 線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- ステップ3701において $x \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ3702において $X_d + T_1$ が計算される。ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d + X_d$ が計算される。その結果がレジスタ T_2 に
- 15 格納される。ステップ3703において $X_d - T_1$ が計算され、ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d - X_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3704においてレジスタ T_3 の2乗が計算される。ここでレジスタ T_3 には $xZ_d - X_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3705
 - 20 において $T_3 \times X_{d+1}$ が計算される。ここでレジスタ T_3 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3706において $x \times X_d$ が計算され、レジスタ T_1 に格納される。ステップ3707において $a \times Z_d$ が計算され、レジスタ T_4 に格納される。ステップ3708において $T_1 + T_4$ が計算される。ここでレジスタ
 - 25 T_1 には xX_d がレジスタ T_4 には aZ_d がそれぞれ格納されており、したがって $xX_d + aZ_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3709において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $xX_d + aZ_d$ がレジスタ T_2 には $xZ_d + X_d$ がそれぞれ格納されており、したがって $(xX_d + aZ_d)(xZ_d + X_d)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3710におい

- てレジスタ Z_d の2乗が計算され、レジスタ T_2 に格納される。ステップ3711において $T_2 \times 2b$ が計算される。ここでレジスタ T_2 には Z_d^2 が格納されており、したがって $2bZ_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3712において $T_1 + T_2$ が計算される。ここでレジスタ T_1 には $(xX_d + aZ_d)(xZ_d + X_d)$ がレジスタ T_2 には $2bZ_d^2$ がそれぞれ格納されており、したがって $(xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3713において $T_1 \times Z_{d+1}$ が計算される。ここでレジスタ T_1 には $(xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2$ が格納されており、したがって $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3714において $T_1 - T_3$ が計算される。ここでレジスタ T_1 には $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2)$ がレジスタ T_3 には $X_{d+1}(X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3715において $2y \times Z_d$ が計算され、レジスタ T_2 に格納される。ステップ3716において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $2yZ_d$ が格納されており、したがって $2yZ_dZ_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3717において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $2yZ_dZ_{d+1}$ が格納されており、したがって $2yZ_dZ_{d+1}Z_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3718においてレジスタ T_3 の逆元が計算される。ここでレジスタ T_3 には $2yZ_dZ_{d+1}Z_d$ が格納されており、したがって $1/2yZ_dZ_{d+1}Z_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3719において $T_1 \times T_3$ が計算される。ここでレジスタ T_1 には $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ がレジスタ T_3 には $1/2yZ_dZ_{d+1}Z_d$ がそれぞれ格納されており、したがって $(Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2) - X_{d+1}(X_d - xZ_d)^2) / 2yZ_dZ_{d+1}Z_d$ が計算される。その結果がレジスタ y_d に格納される。ステップ3720において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $2yZ_dZ_{d+1}$ が格納されており、したがって $2yZ_dZ_{d+1}X_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3721において $T_2 \times T_3$ が計算される。ここでレジ

スタ T_2 には $2yZ_dZ_{d+1}X_d$ がレジスタ T_3 には $1/2yZ_dZ_{d+1}Z_d$ がそれぞれ格納されており、したがって $2yZ_dZ_{d+1}X_d/2yZ_dZ_{d+1}Z_d$ が計算される。その結果がレジスタ x_d に格納される。したがってレジスタ x_d には $2yZ_dZ_{d+1}X_d/2yZ_dZ_{d+1}Z_d$ が格納されている。レジスタ y_d にはステップ3719において $(Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2)-X_{d+1}(X_d-xZ_d)^2)/2yZ_dZ_{d+1}Z_d$ が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により、与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} からワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数27を得る。点 P 及び点 dP はワイエルシュトラス型楕円曲線上の点であるので、 $y_d^2=x_d^3+ax_d+b$ 及び $y^2=x^3+ax+b$ をみたす。数27に代入し、 y_d^2 及び y^2 を消去し、式を整理すると、

$$y_d=\{(x_dx+a)(x_d+x)+2b-(x_d-x)^2x_{d+1}\}/(2y) \quad \cdots \text{数70}$$

15 を得る。ここで $x_d=X_d/Z_d$ 、 $x_{d+1}=X_{d+1}/Z_{d+1}$ であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d=\{Z_{d+1}((X_dx+aZ_d)(X_d+xZ_d)-2bZ_d^2)-(X_d-xZ_d)^2X_{d+1}\}/(2yZ_dZ_{d+1}Z_d) \quad \cdots \text{数71}$$

20 $x_d=X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d の分母と通分することにより、

$$x_d=(2yZ_dZ_{d+1}X_d)/(2yZ_dZ_{d+1}Z_d) \quad \cdots \text{数72}$$

となる。ここで、 x_d 、 y_d は図37で示した処理により与えられる。したがって、アフィン座標 (x_d, y_d) の値が全て復元されていることになる。

上記手順はステップ3701、ステップ3705、ステップ3706、ステップ3707、ステップ3709、ステップ3710、ステップ3711、ステップ3713、ステップ3715、ステップ3716、ステップ3717、ステップ3719、ステップ3720及びステップ3721において有限体上の乗算の計算量を必要とする。また、ステップ3704において有限体上の2乗算の計算量を必要とする。また、ステップ3718において有限体上の逆元演算の計算量

を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の2乗算の計算量を S 及び有限体上の逆元演算の計算量を I とすると、上記手順は $14M + S + I$ の計算量を必要とする。

- 5 これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が160ビットであれば、高速スカラー倍計算の計算量はおおよそ1500 M 弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は54.8 M であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。
- 10 尚、上記手順をとらなくても、上記計算式により与えられた x_d 、 y_d の値が計算できれば x_d 、 y_d の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。

次に図44により、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力する高速スカラー倍計算部の処理について説明する。

- 15 高速スカラー倍計算部202では、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P を入力し、以下の手順によりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ のうち X_{d+1} 及び Z_{d+1} を出力する。ステップ4416として、与えられたワイエルシュトラス型楕円曲線上の点 P をモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点 P とする。ステップ4401として、変数 I に初期値1を代入する。ステップ4402として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点 $2P$ を計算する。ステップ4403として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ4402で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ4404として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すれ

ばステップ4 4 1 5へ行く。一致しなければステップ4 4 0 5へ行く。ステップ
 4 4 0 5として、変数 I を1増加させる。ステップ4 4 0 6として、スカラー値
 の I 番目のビットの値が0であるか1であるかを判定する。そのビットの値が0
 5 0へ行く。ステップ4 4 0 7として、射影座標により表された点の組
 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算す
 る。その後ステップ4 4 0 8へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型
 楕円曲線の射影座標における加算公式を用いて計算される。ステップ4 4 0 8と
 して、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行
 10 ない、点 $2mP$ を計算する。その後ステップ4 4 0 9へ行く。ここで、2倍算 $2(mP)$
 は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。
 ステップ4 4 0 9として、ステップ4 4 0 8で求めた点 $2mP$ とステップ4 4 0 7
 で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代
 わりに格納する。その後ステップ4 4 0 4へ戻る。ここで、点 $2mP$ 、点 $(2m+$
 15 $1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ4 4
 1 0として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$
 の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ4 4 1 1へ
 行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加
 算公式を用いて計算される。ステップ4 4 1 1として、射影座標により表された
 20 点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計
 算する。その後ステップ4 4 1 2へ行く。ここで、2倍算 $2((m+1)P)$ は、モンゴ
 メリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ
 4 4 1 2として、ステップ4 4 1 0で求めた点 $(2m+1)P$ とステップ4 4 1 1で求
 めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わり
 25 に格納する。その後ステップ4 4 0 4へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、
 点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ4 4 1 5とし
 て、モンゴメリ型楕円曲線における点 $(m-1)P$ を、ワイエルシュトラス型楕円曲線
 上で射影座標により表された点に変換する。その点の X 座標及び Z 座標をそれぞれ
 あらためて X_{m-1} 及び Z_{m-1} とおく。また、モンゴメリ型楕円曲線において射影座標

- で表された点の組(mP , $(m+1)P$)に対して、点 mP 及び点 $(m+1)P$ をワイエルシュトラス型楕円曲線上で射影座標で表された点に変換し、それぞれ $mP = (X_m, Y_m, Z_m)$ 及び $(m+1)P = (X_{m+1}, Y_{m+1}, Z_{m+1})$ とあらためて置き直す。ここで、 Y_m 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び2倍算の公式
- 5 では Y 座標を求める事ができないので、求まっていない。ステップ4413として、ワイエルシュトラス型楕円曲線上で射影座標で表された点 $mP = (X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d として、ワイエルシュトラス型楕円曲線上で射影座標で表された点 $(m+1)P = (X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} として、出力する。また上記手順により、 m
- 10 とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ ととることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M+2S$ である。スカラー値の I 番目のビットの値が0であれば、ステップ4407において加算の計算量、ステップ4408において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ4410において加算の計算量、ステップ4411において2倍算の計算量が必要となる。すなわち $6M+4S$ の
- 15 計算量が必要である。いずれの場合においても $6M+4S$ の計算量が必要である。ステップ4404、ステップ4405、ステップ4406、ステップ4407、ステップ4408、ステップ4409乃至はステップ4404、ステップ4405、ステップ4406、ステップ4410、ステップ4411、ステップ4412の繰り返しの回数は、(スカラー値 d のビット長) - 1回となるので、ステップ4402での2倍算の計算量とステップ4416でのモンゴメリ型楕円曲線上の点への変換に必要な計算量及びステップ4415でのワイエルシュトラス型楕円曲線上の点への変換に必要な計算量を考慮に入れると、全体の計算量は $(6M+4S)k+2M-2S$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S=0.8M$ 程度と見積もられるので、全体の計算量は
- 25

おおよそ $(9.2k + 0.4)M$ となる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、上記手順のアルゴリズムの計算量はおおよそ 1472 M となる。スカラー値 d のビットあたりの計算量としてはおおよそ $9.2M$ となる。

A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ $10M$ と見積もられる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算方法の計算量はおおよそ $1600M$ となる。したがって、上記本発明による手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $14M + S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 0.4)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M$ 、 $S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 55.2)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量はおおよそ $1527M$ となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおおよそ $1640M$ であり、これと比べて必要となる計算量は削減されている。

第 18 の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたもの

- である。すなわち、スカラー倍計算部 103 の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部 103 の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部 103 がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標 X_d, Y_d 及び Z_d の復元を行なう。スカラー倍計算部 103 は射影座標において完全に座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を計算結果として出力する。
- 次に図 38 により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に X_d, Y_d, Z_d を出力する座標復元部の処理について説明する。
- 座標復元部 203 では、ワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部 103 に入力されたワイエルシュトラス型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順で射影座標において完全な座標が与えられたスカラー倍点 (X_d, Y_d, Z_d) を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d として

ワイエルシュトラス型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- 5 ステップ3801において $x \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ3802において $X_d + T_1$ が計算される。ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d + X_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3803において $X_d - T_1$ が計算され、ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d - X_d$ が計算される。その結果が
- 10 レジスタ T_3 に格納される。ステップ3804においてレジスタ T_3 の2乗が計算される。ここでレジスタ T_3 には $xZ_d - X_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ3805において $T_3 \times X_{d+1}$ が計算される。ここでレジスタ T_3 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ
- 15 T_3 に格納される。ステップ3806において $x \times X_d$ が計算され、レジスタ T_1 に格納される。ステップ3807において $a \times Z_d$ が計算され、レジスタ T_4 に格納される。ステップ3808において $T_1 + T_4$ が計算される。ここでレジスタ T_1 には xX_d がレジスタ T_4 には aZ_d がそれぞれ格納されており、したがって $xX_d + aZ_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ38
- 20 09において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $xX_d + aZ_d$ がレジスタ T_2 には $xZ_d + X_d$ がそれぞれ格納されており、したがって $(xX_d + aZ_d)(xZ_d + X_d)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3810においてレジスタ Z_d の2乗が計算され、レジスタ T_2 に格納される。ステップ3811において $T_2 \times 2b$ が計算される。ここでレジスタ T_2 には Z_d^2 が格納されて
- 25 しており、したがって $2bZ_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ3812において $T_1 + T_2$ が計算される。ここでレジスタ T_1 には $(xX_d + aZ_d)(xZ_d + X_d)$ がレジスタ T_2 には $2bZ_d^2$ がそれぞれ格納されており、したがって $(xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3813において $T_1 \times Z_{d+1}$ が計算される。ここでレ

- レジスタ T_1 には $(xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2$ が格納されており、したがって $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 3814 において $T_1 - T_3$ が計算される。ここでレジスタ T_1 には $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2)$ がレジスタ T_3 には $X_{d+1}(X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ が計算される。その結果がレジスタ Y_d に格納される。ステップ 3815 において $2y \times Z_d$ が計算され、レジスタ T_2 に格納される。ステップ 3816 において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $2yZ_d$ が格納されており、したがって $2yZ_dZ_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 3817 において $T_2 \times X_d$ が計算される。ここでレジスタ T_2 には $2yZ_dZ_{d+1}$ が格納されており、したがって $2yZ_dZ_{d+1}X_d$ が計算される。その結果がレジスタ X_d に格納される。ステップ 3819 において $T_2 \times Z_d$ が計算される。ここでレジスタ T_2 には $2yZ_dZ_{d+1}$ が格納されており、したがって $2yZ_dZ_{d+1}Z_d$ が計算される。その結果がレジスタ Z_d に格納される。したがってレジスタ Z_d には $2yZ_dZ_{d+1}Z_d$ が格納されている。レジスタ Y_d にはステップ 3814 において $Z_{d+1}((xX_d + aZ_d)(xZ_d + X_d) + 2bZ_d^2) + X_{d+1}(X_d - xZ_d)^2$ が格納され、その後更新が行なわれないので、その値が保持されている。レジスタ X_d にはステップ 3817 において $2yZ_dZ_{d+1}X_d$ が格納され、その後更新が行なわれないので、その値が保持されている。
- 20 上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標 (X_d, Y_d, Z_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数 27 を得る。点 P 及び点 dP はワイエルシュトラス型楕円曲線上の点であるので、 $y_d^2 = x_d^3 + ax_d + b$ 及び $y^2 = x^3 + ax + b$ をみたとす。数 27 に代入し、 y_d^2 及び y^2 を消去し、式を整理すると、数 70 を得る。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} = X_{d+1}/Z_{d+1}$ であり、この値を代入することにより射影座標の値へと変換すると、数 71 を得る。 $x_d = X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d の分母と通分することにより、数 72 となる。その結果として

$$Y_d = Z_{d+1} [(X_d x + a Z_d) (X_d + x Z_d) + 2b Z_d^2] - (X_d - x Z_d)^2 X_{d+1} \quad \cdots \text{数 7 3}$$

とし、 X_d 及び Z_d をそれぞれ

$$2y Z_d Z_{d+1} X_d \quad \cdots \text{数 7 4}$$

$$2y Z_d Z_{d+1} Z_d \quad \cdots \text{数 7 5}$$

- 5 により更新すればよい。ここで、 X_d , Y_d , Z_d は図 3 8 で示した処理により与えられる。したがって、射影座標 (X_d, Y_d, Z_d) の値は全て復元されたことになる。

- 上記手順はステップ 3 8 0 1、ステップ 3 8 0 5、ステップ 3 8 0 6、ステップ 3 8 0 7、ステップ 3 8 0 9、ステップ 3 8 1 1、ステップ 3 8 1 3、ステップ 3 8 1 5、ステップ 3 8 1 6、ステップ 3 8 1 7 及びステップ 3 8 1 8 において有限体上の乗算の計算量を必要とする。また、ステップ 3 8 0 4 およびステップ 3 8 1 0 において有限体上の 2 乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S とすると、上記手順は $11M + 2S$ の計算量を必要とする。これは高速
- 15 スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 1 6 0 ビットであれば、高速スカラー倍計算の計算量はおおよそ $1500M$ 弱と見積もられる。 $S = 0.8M$ と仮定すると座標復元の計算量は $12.6M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

- 20 尚、上記手順をとらなくても、上記計算式により与えられた X_d, Y_d, Z_d の値が計算できれば X_d, Y_d, Z_d の値が復元できる。また、 x_d, y_d が上記計算式により与えられる値を取るように X_d, Y_d, Z_d の値を選択し、その値が計算できれば X_d, Y_d, Z_d が復元できる。それらの場合においては一般的に復元に必要となる計算量が增大する。

- 25 次に、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力するアルゴリズムについて説明する。

第 1 8 実施例の高速スカラー倍計算部 2 0 2 の高速スカラー倍計算方法として、第 1 7 実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力

するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくても、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $11M + 2S$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 0.4)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 13)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量はおよそ 1485M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要な計算量はおよそ 1600M であり、これと比べて必要となる計算量は削減されている。

第 19 の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部 103 の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部 103 の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部 103 がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標の

うち x_d 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d-1)P = (x_{d-1}, y_{d-1})$ の座標のうち x_{d-1} を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点 $P = (x, y)$

- 5 と共にその情報を座標復元部203に与える。座標復元部203は与えられた座標の値 x_d 、 x_{d+1} 、 x_{d-1} 、 x 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標 y_d の復元を行なう。スカラー倍計算部103はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。

- 10 次に図39により、座標 x 、 y 、 x_d 、 x_{d+1} が与えられた場合に、 x_d 、 y_d を出力する座標復元部の処理について説明する。

座標復元部203では、ワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち

- 15 x_{d+1} 、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。

- ステップ3901において $x_d \times x$ が計算され、レジスタ T_1 に格納される。ステップ3902において $T_1 + a$ が計算される。ここでレジスタ T_1 には $x_d x$ が格納されており、したがって $x_d x + a$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3903において $x_d + x$ が計算され、レジスタ T_2 に格納される。ステップ3904において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $x_d x + a$ がレジスタ T_2 には $x_d + x$ がそれぞれ格納されており、したがって $(x_d x + a)(x_d + x)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ
- 25 3905において $T_1 + 2b$ が計算される。ここでレジスタ T_1 には $(x_d x + a)(x_d + x)$ が格納されており、したがって $(x_d x + a)(x_d + x) + 2b$ が計算される。その結果がレジスタ T_1 に格納される。ステップ3906において $x_d - x$ が計算され、レジスタ T_2 に格納される。ステップ3907において T_2 の2乗が計算される。ここでレジスタ T_2 には $x_d - x$ が格納されており、したがって $(x_d - x)^2$ が計算さ

れる。その結果がレジスタ T_2 に格納される。ステップ 3908 において $T_2 \times x_{d+1}$ が計算される。ここでレジスタ T_2 には $(x_d - x)^2$ が格納されており、したがって $x_{d+1} (x_d - x)^2$ が計算される。その結果がレジスタ T_2 に格納される。

ステップ 3909 において $T_1 - T_2$ が計算される。ここでレジスタ T_1 には

- 5 $(x_d x + a)(x_d + x) + 2b$ がレジスタ T_2 には $x_{d+1} (x_d - x)^2$ がそれぞれ格納されており、したがって $(x_d x + a)(x_d + x) + 2b - x_{d+1} (x_d - x)^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 3910 において $2y$ の逆元が計算され、レジスタ T_2 に格納される。ステップ 3911 において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(x_d x + a)(x_d + x) + 2b - x_{d+1} (x_d - x)^2$ がレジスタ T_2 には $1/2y$ がそれぞれ格納されており、したがって $((x_d x + a)(x_d + x) + 2b - x_{d+1} (x_d - x)^2)/2y$ が計算される。その結果がレジスタ y_d に格納される。したがってレジスタ y_d には $((x_d x + a)(x_d + x) + 2b - x_{d+1} (x_d - x)^2)/2y$ が格納されている。レジスタ x_d は全く更新されないので入力された値が保持されている。
- 10

上記手順によりスカラー倍点の y 座標 y_d が復元される理由は以下の通りである。

- 15 点 $(d+1)P$ は点 dP に点 P を加算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数 27 を得る。点 P 及び点 dP はワイエルシュトラス型楕円曲線上の点であるので、 $y_d^2 = x_d^3 + ax_d + b$ 及び $y^2 = x^3 + ax + b$ をみたす。数 27 に代入し、 y_d^2 及び y^2 を消去し、式を整理すると、数 70 を得る。ここで x_d, y_d は図 39 の処理によって与えられる。したがって、アフィン座標 (x_d, y_d) の値を全て復元していることになる。
- 20

- 上記手順はステップ 3901、ステップ 3904、ステップ 3908 及びステップ 3911 において有限体上の乗算の計算量を必要とする。また、ステップ 3907 において有限体上の 2 乗算の計算量を必要とする。さらにステップ 3910 において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S 、有限体上の逆元演算の計算量を I とすると、上記手順は
- 25 $4M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 160 ビットであれば、高速スカラー

倍計算の計算量はおよそ1500M弱と見積もられる。 $S=0$ 、8M及び $I=40M$ と仮定すると座標復元の計算量は44.8Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

- 5 尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば y_d の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。

次に図44により、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 x_d 、 x_{d+1} を出力するアルゴリズムについて説明する。

- 高速スカラー倍計算部202では、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点 P を入力し、以下の手順によりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP=(x_d, y_d)$ のうち x_d 、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点 $(d+1)P=(x_{d+1}, y_{d+1})$ のうち x_{d+1} を出力する。ステップ4416として、与えられたワイエルシュトラス型楕円曲線上の点 P をモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点 P とする。ステップ4401として、変数 I に初期値1を代入する。ステップ4402として、点 P の2倍点 $2P$ を計算する。ここで点 P は射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点 $2P$ を計算する。ステップ4403として、スカラー倍計算部103に入力された楕円曲線上の点 P とステップ4402で求めた点 $2P$ を、点の組 $(P, 2P)$ として格納する。ここで点 P 及び点 $2P$ は射影座標で表されている。ステップ4404として、変数 I とスカラー値 d のビット長とが一致するかどうかを判定し、一致すればステップ4415へ行く。一致しなければステップ4405へ行く。ステップ4405として、変数 I を1増加させる。ステップ4406として、スカラー値の I 番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ4406へ行く。そのビットの値が1であればステップ4410へ行く。ステップ4407として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ4408へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標にお

- る加算公式を用いて計算される。ステップ4408として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP の2倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ4409へ行く。ここで、2倍算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて計算される。ステップ4409として、
- 5 ステップ4408で求めた点 $2mP$ とステップ4407で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ4404へ戻る。ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ4410として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点
- 10 $(2m+1)P$ を計算する。その後ステップ4411へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ4411として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の2倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ4412へ行く。ここで、2倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標に
- 15 おける2倍算の公式を用いて計算される。ステップ4412として、ステップ4410で求めた点 $(2m+1)P$ とステップ4411で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ4404へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ4415として、モンゴメリ型楕円
- 20 曲線において射影座標で表された点の組 $(mP, (m+1)P)$ に対して、点 mP 及び点 $(m+1)P$ をワイエルシュトラス型楕円曲線上でアフィン座標で表された点に変換し、それぞれ $mP = (x_m, y_m)$ 及び $(m+1)P = (x_{m+1}, y_{m+1})$ とあらためて置き直す。ここで、 y_m 及び y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び2倍算の公式ではY座標を求める事ができないので、求まっていない。その
- 25 後ステップ4413へ行く。ステップ4413として、ワイエルシュトラス型楕円曲線上で射影座標で表された点 $mP = (x_m, y_m)$ より x_m を x_d として、ワイエルシュトラス型楕円曲線上でアフィン座標で表された点 $(m+1)P = (x_{m+1}, y_{m+1})$ より x_{m+1} を x_{d+1} として、出力する。また上記手順により、 m とスカラー値 d はビット長が等しくさらにそのビットのパターンも同じとなる為、等し

くなる。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1 = 1$ とすることにより $3M + 2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の公式の計算量は、 $3M + 2S$ である。スカラー値の I 番目のビットの値が0であれば、ステップ4407において加算の計算量、ステップ4408において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ4410において加算の計算量、ステップ4411において2倍算の計算量が必要となる。すなわち $6M + 4S$ の計算量が必要である。いずれの場合においても $6M + 4S$ の計算量が必要である。ステップ4404、ステップ4405、ステップ4406、ステップ4407、ステップ4408、ステップ4409乃至はステップ4404、ステップ4405、ステップ4406、ステップ4410、ステップ4411、ステップ4412の繰り返しの回数は、(スカラー値 d のビット長) - 1 回となるので、
- ステップ4402での2倍算の計算量とステップ4416でのモンゴメリ型楕円曲線上への点への変換に必要な計算量及びステップ4415でのワイエルシュトラス型楕円曲線上の点への必要な計算量を考慮に入れると、全体の計算量は $(6M + 4S)k + 4M - 2S + I$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S = 0.8M$ 程度、計算量 I は、 $I = 40M$ 程度と見積もられるので、全体の計算量はおおよそ $(9.2k + 42.4)M$ となる。例えばスカラー値 d が160ビット ($k = 160$) であれば、上記手順のアルゴリズムの計算量はおおよそ $1514M$ となる。スカラー値 d のビットあたりの計算量としてはおおよそ $9.2M$ となる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ $10M$ と見積もられる。例えばスカラー値 d が160ビット (k

= 160) であれば、このスカラー倍計算方法の計算量はおおよそ 1640M となる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部 202 において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 x_d ,

- 5 $x_{d+1}, x_d=1$ を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- スカラー倍計算部 103 における座標復元部 203 の座標復元に必要な計算量は $4M + S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k + 42.4)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M$ 、 $S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 87.2)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量は 1559M となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおおよそ 1640M であり、これと比べて必要となる計算量は削減されている。
- 10
15

- 第 20 の実施例は、入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部 103 がスカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d, y_d) を計算し出力するものである。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P =$
- 20
25

- ($X_{d+1}, Y_{d+1}, Z_{d+1}$)の座標のうち X_{d+1} 及び Z_{d+1} を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たに $P=(x, y)$ とおく。高速スカラー倍計算部202は、 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y を座標復元部203に与える。座標復元部203は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP=(x_d, y_d)$ の座標 x_d 及び y_d の復元を行なう。スカラー倍計算部103はアフィン座標において完全に座標が与えられたスカラー倍点 (x_d, y_d) を計算結果として出力する。
- 10 次に図40により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に x_d, y_d を出力する座標復元部の処理について説明する。

- 座標復元部203では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ の座標うち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d, y_d) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線における
- 15 スカラー倍点 dP のアフィン座標を $(x_d^{\text{Mon}}, y_d^{\text{Mon}})$ で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- ステップ4001において $x \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ4002において $X_d + T_1$ が計算される。ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d + X_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4003において $X_d - T_1$ が計算され、ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d - X_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ4004においてレジスタ T_3 の2乗が計算される。ここでレジスタ T_3 には $xZ_d - X_d$ が格納されており、したがって $(X_d -$
- 25

- $xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ4005において $T_3 \times X_{d+1}$ が計算される。ここでレジスタ T_3 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1}(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ4006において $2A \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ4007において $T_2 + T_1$ が計算される。ここでレジスタ T_2 には $xZ_d + X_d$ がレジスタ T_1 には $2AZ_d$ がそれぞれ格納されており、したがって $xZ_d + X_d + 2AZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4008において $x \times X_d$ が計算され、レジスタ T_4 に格納される。ステップ4009において $T_4 + Z_d$ が計算される。ここでレジスタ T_4 には xX_d が格納されており、したがって $xX_d + Z_d$ が計算される。その結果がレジスタ T_4 に格納される。ステップ4010において $T_2 \times T_4$ が計算される。ここでレジスタ T_2 には $xZ_d + X_d + 2AZ_d$ がレジスタ T_4 には $xX_d + Z_d$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4011において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2AZ_d$ が格納されており、したがって $2AZ_d^2$ が計算される。その結果がレジスタ T_1 に格納される。ステップ4012において $T_2 - T_1$ が計算される。ここでレジスタ T_2 には $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ がここでレジスタ T_1 には $2AZ_d^2$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4013において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2$ が格納されており、したがって $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4014において $T_2 - T_3$ が計算される。ここでレジスタ T_2 には $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ がレジスタ T_3 には $X_{d+1}(X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4015において $2B \times y$ が計算され、レジスタ T_1 に格納される。ステップ4016において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2By$ が格納されており、したがって $2ByZ_d$ が計算される。その結果がレジスタ

T_1 に格納される。ステップ4017において $T_1 \times Z_{d+1}$ が計算される。ここでレジスタ T_1 には $2ByZ_d$ が格納されており、したがって $2ByZ_d Z_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ4018において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1}$ が格納されており、したがって $2ByZ_d Z_{d+1} Z_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ4019において $T_3 \times s$ が計算される。ここでレジスタ T_3 には $2ByZ_d Z_{d+1} Z_d$ が格納されており、したがって $2ByZ_d Z_{d+1} Z_d s$ が計算される。その結果がレジスタ T_3 に格納される。ステップ4020においてレジスタ T_3 の逆元が計算される。ここでレジスタ T_3 には $2ByZ_d Z_{d+1} Z_d s$ が格納されており、したがって $1/2ByZ_d Z_{d+1} Z_d s$ が計算される。その結果がレジスタ T_3 に格納される。ステップ4021において $T_2 \times T_3$ が計算される。ここでレジスタ T_2 には $Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1} (X_d - xZ_d)^2$ がレジスタ T_3 には $1/2ByZ_d Z_{d+1} Z_d s$ がそれぞれ格納されており、したがって $\{Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1} (X_d - xZ_d)^2\} / 2ByZ_d Z_{d+1} Z_d s$ が計算される。その結果がレジスタ y_d に格納される。ステップ4022において $T_1 \times X_d$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1}$ が格納されており、したがって $2ByZ_d Z_{d+1} X_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ4023において $T_1 \times T_3$ が計算される。ここでレジスタ T_1 には $2ByZ_d Z_{d+1} X_d$ がレジスタ T_3 には $1/2ByZ_d Z_{d+1} Z_d s$ がそれぞれ格納されており、したがって $2ByZ_d Z_{d+1} X_d / 2ByZ_d Z_{d+1} Z_d s (=X_d / Z_d s)$ が計算される。その結果が T_1 に格納される。ステップ4024において $T_1 + \alpha$ が計算される。ここでレジスタ T_1 には $X_d / Z_d s$ が格納されており、したがって $(X_d / Z_d s) + \alpha$ が計算される。その結果が x_d に格納される。したがってレジスタ x_d には $(X_d / Z_d s) + \alpha$ の値が格納されている。 y_d にはステップ4021において $\{Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1} (X_d - xZ_d)^2\} / 2ByZ_d Z_{d+1} Z_d s$ が格納され、その後更新が行なわれないので、その値が保持されている。その結果として、ワイエルシュトラス型楕円曲線におけるアフィン座標 (x_d, y_d) の値が全て復元されている。

上記手順により与えられた x 、 y 、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} からワイエルシ

シュトラス型楕円曲線におけるスカラー倍点のアフィン座標 (x_d, y_d) における値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数38を得る。点 P 及び点 dP はモンゴメリ型楕円曲線上の点であるので、

- 5 $By_d^{Mon2} = x_d^{Mon3} + Ax_d^{Mon2} + x_d^{Mon}$ 及び $By_d^2 = x^3 + Ax^2 + x$ をみたとす。数38に代入し、 By_d^{Mon2} 及び By_d^2 を消去し、式を整理すると、

$$y_d^{Mon} = \{(x_d^{Mon} x + 1)(x_d^{Mon} + x + 2A) - 2A - (x_d^{Mon} - x)^2 x_{d+1}\} / (2By_d) \quad \cdots \text{数76}$$

を得る。ここで $x_d^{Mon} = X_d / Z_d$ 、 $x_{d+1} = X_{d+1} / Z_{d+1}$ であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

- 10 $y_d^{Mon} = \{Z_{d+1}((X_d x + Z_d)(X_d + x Z_d + 2AZ_d) - 2AZ_d^2) - (x_d - x Z_d)^2 X_{d+1}\} / (2By_d Z_d Z_{d+1} Z_d) \quad \cdots \text{数77}$

$x_d^{Mon} = X_d / Z_d$ であるが、逆元演算の回数を減らす目的で y_d^{Mon} の分母と通分することにより、

$$x_d^{Mon} = (2By_d Z_d Z_{d+1} X_d) / (2By_d Z_d Z_{d+1} Z_d) \quad \cdots \text{数78}$$

- 15 となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp.238-257 に記載されている。それによると、変換パラメタを s, α として、 $y_d = s^{-1} y_d^{Mon}$ 及び $x_d = s^{-1} x_d^{Mon} + \alpha$ の
20 関係がある。結果として数79、数80を得る。

$$y_d = \{Z_{d+1}((X_d x + Z_d)(X_d + x Z_d + 2AZ_d) - 2AZ_d^2) - (x_d - x Z_d)^2 X_{d+1}\} / (2sBy_d Z_d Z_{d+1} Z_d) \quad \cdots \text{数79}$$

$$x_d = ((2By_d Z_d Z_{d+1} X_d) / (2sBy_d Z_d Z_{d+1} Z_d)) + \alpha \quad \cdots \text{数80}$$

- ここで、 x_d, y_d は図40より与えられる。したがって、ワイエルシュトラス
25 型楕円曲線におけるアフィン座標 (x_d, y_d) の値が全て復元されていることになる。

上記手順はステップ4001、ステップ4005、ステップ4006、ステップ4008、ステップ4010、ステップ4011、ステップ4013、ステップ4015、ステップ4016、ステップ4017、ステップ4018、ステッ

プ4019、ステップ4021、ステップ4022及びステップ4023において有限体上の乗算の計算量を必要とする。また、ステップ4004において有限体上の2乗算の計算量を必要とする。また、ステップ4020において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の2乗算の計算量を S 及び有限体上の逆元演算の計算量を I とすると、上記手順は $15M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が160ビットであれば、高速スカラー倍計算の計算量はおよそ1500 M 弱と見積もられる。 $S = 0.8M$ 、 $I = 40M$ と仮定すると座標復元の計算量は $55.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた x_d 、 y_d の値が計算できれば x_d 、 y_d の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタである A 乃至は B の値やモンゴメリ型楕円曲線への変換パラメタである s を小さくすることにより、ステップ4006乃至はステップ4015における乗算の計算量やステップ4019における乗算の計算量を削減することができる。

次に、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力する高速スカラー倍計算部の処理について説明する。

この場合、第20実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、第9実施例の高速スカラー倍計算方法（図8参照）を用いる。これにより、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部202において上記アルゴリズムを用いなくても、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 X_d 、 Z_d 、 X_{d+1} 、 Z_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

スカラー倍計算部103における座標復元部203の座標復元に必要な計算量

は $1.5M + S + I$ であり、これは高速スカラー倍計算部 202 の高速スカラー倍計算に必要な計算量の $(9.2k - 3.6)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部 103 のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40$
 5 M 、 $S = 0.8M$ と仮定すると、この計算量はおよそ $(9.2k + 52.2)M$ と見積もることができる。例えばスカラー値 d が 160 ビット ($k = 160$) であれば、このスカラー倍計算に必要な計算量は $1524M$ となる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍
 10 点をアフィン座標として出力する場合に必要な計算量はおよそ $1640M$ であり、これと比べて必要となる計算量は削減されている。

第 21 の実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部 103 がスカラー
 15 値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点、 (X_d^W, Y_d^W, Z_d^W) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部 103 に入力すると高速スカラー倍計算部 202 がそれを受け取る。高速スカラー倍計算部 202 は受け取ったスカラー値 d
 20 と与えられたワイエルシュトラス型楕円曲線上の点 P からモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点 P を、与えられたワイエルシュトラス型楕円
 25 曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たに $P = (x, y)$ とおく。高速スカラー倍計算部 202 は、 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y を座標復元部 203 に与える。座標復元部 203 は与えられた座標の値 $X_d, Z_d, X_{d+1}, Z_{d+1}, x$ 及び y よりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点 $dP = (X_d^W, Y_d^W, Z_d^W)$ の座標 X_d^W, Y_d^W 及び Z_d^W の

復元を行なう。スカラー倍計算部 103 は射影座標において完全に座標が与えられたスカラー倍点 (X_d^W, Y_d^W, Z_d^W) を計算結果として出力する。

次に図 41 により、座標 $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ が与えられた場合に X_d^W, Y_d^W, Z_d^W を出力する座標復元部の処理について説明する。

- 5 座標復元部 203 では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点 $dP=(X_d, Y_d, Z_d)$ の座標のうち X_d 及び Z_d 、射影座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち X_{d+1} 及び Z_{d+1} 、スカラー倍計算部 103 に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でワイエルシュトラス型楕円
- 10 曲線上で射影座標において完全な座標が与えられたスカラー倍点 (X_d^W, Y_d^W, Z_d^W) を出力する。ここで入力されたモンゴメリ型楕円曲線上の点 P のアフィン座標を (x, y) で、射影座標を (X_1, Y_1, Z_1) でそれぞれ表す。入力されたスカラー値を d としてモンゴメリ型楕円曲線におけるスカラー倍点 dP のアフィン座標を (x_d, y_d) で、射影座標を (X_d, Y_d, Z_d) でそれぞれ表す。モンゴメリ型楕円曲線上
- 15 の点 $(d+1)P$ のアフィン座標を (x_{d+1}, y_{d+1}) で、射影座標を $(X_{d+1}, Y_{d+1}, Z_{d+1})$ でそれぞれ表す。

- ステップ 4101 において $x \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ 4102 において $X_d + T_1$ が計算される。ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d + X_d$ が計算される。その結果がレジスタ T_2 に
- 20 格納される。ステップ 4103 において $X_d - T_1$ が計算され、ここでレジスタ T_1 には xZ_d が格納されており、したがって $xZ_d - X_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 4104 においてレジスタ T_3 の 2 乗が計算される。ここでレジスタ T_3 には $xZ_d - X_d$ が格納されており、したがって $(X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 4105
 - 25 において $T_3 \times X_{d+1}$ が計算される。ここでレジスタ T_3 には $(X_d - xZ_d)^2$ が格納されており、したがって $X_{d+1} (X_d - xZ_d)^2$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 4106 において $2A \times Z_d$ が計算され、レジスタ T_1 に格納される。ステップ 4107 において $T_2 + T_1$ が計算される。ここでレジスタ T_2 には $xZ_d + X_d$ がレジスタ T_1 には $2AZ_d$ がそれぞれ格納されており、した

- がって $xZ_d + X_d + 2AZ_d$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 4 1 0 8 において $x \times X_d$ が計算され、レジスタ T_4 に格納される。ステップ 4 1 0 9 において $T_4 + Z_d$ が計算される。ここでレジスタ T_4 には xX_d が格納されており、したがって $xX_d + Z_d$ が計算される。その結果がレジスタ T_4 に格納
- 5 される。ステップ 4 1 1 0 において $T_2 \times T_4$ が計算される。ここでレジスタ T_2 には $xZ_d + X_d + 2AZ_d$ がレジスタ T_4 には $xX_d + Z_d$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 4 1 1 1 において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2AZ_d$ が格納されており、したがって $2AZ_d^2$ が計算される。その結果
- 10 がレジスタ T_1 に格納される。ステップ 4 1 1 2 において $T_2 - T_1$ が計算される。ここでレジスタ T_2 には $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d)$ がここでレジスタ T_1 には $2AZ_d^2$ がそれぞれ格納されており、したがって $(xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 4 1 1 3 において $T_2 \times Z_{d+1}$ が計算される。ここでレジスタ T_2 には $(xZ_d + X_d +$
- 15 $2AZ_d)(xX_d + Z_d) - 2AZ_d^2$ が格納されており、したがって $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ が計算される。その結果がレジスタ T_2 に格納される。ステップ 4 1 1 4 において $T_2 - T_3$ が計算される。ここでレジスタ T_2 には $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2)$ がレジスタ T_3 には $X_{d+1}(X_d - xZ_d)^2$ がそれぞれ格納されており、したがって $Z_{d+1}((xZ_d + X_d + 2AZ_d)(xX_d +$
- 20 $Z_d) - 2AZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ が計算される。その結果がレジスタ Y_d^W に格納される。ステップ 4 1 1 5 において $2B \times y$ が計算され、レジスタ T_1 に格納される。ステップ 4 1 1 6 において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2By$ が格納されており、したがって $2ByZ_d$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 4 1 1 7 において $T_1 \times Z_{d+1}$ が計算される。こ
- 25 でレジスタ T_1 には $2ByZ_d$ が格納されており、したがって $2ByZ_dZ_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ 4 1 1 8 において $T_1 \times Z_d$ が計算される。ここでレジスタ T_1 には $2ByZ_dZ_{d+1}$ が格納されており、したがって $2ByZ_dZ_{d+1}Z_d$ が計算される。その結果がレジスタ T_3 に格納される。ステップ 4 1 1 9 において $T_3 \times s$ が計算される。ここでレジスタ T_3 には

$2By_d Z_{d+1} Z_d$ が格納されており、したがって $2By_d Z_{d+1} Z_d s$ が計算される。
 その結果がレジスタ Z_d^W に格納される。ステップ 4 1 2 0 において $T_1 \times X_d$ が
 計算される。ここでレジスタ T_1 には $2By_d Z_{d+1}$ が格納されており、したがっ
 て $2By_d Z_{d+1} X_d$ が計算される。その結果がレジスタ T_1 に格納される。ステッ
 5 プ 4 1 2 1 において $Z_d^W \times \alpha$ が計算される。ここでレジスタ Z_d^W には $2By_d$
 $Z_{d+1} Z_d s$ が格納されており、したがって $2By_d Z_{d+1} Z_d s \alpha$ が計算される。そ
 の結果が T_3 に格納される。ステップ 4 1 2 2 において $T_1 + T_3$ が計算される。
 ここでレジスタ T_1 には $2By_d Z_{d+1} X_d$ がレジスタ T_3 には $2By_d Z_{d+1} Z_d s \alpha$ が
 それぞれ格納されており、したがって $2By_d Z_{d+1} X_d + 2By_d Z_{d+1} Z_d s \alpha$ が計算
 10 される。その結果が X_d^W に格納される。したがってレジスタ x_d には $2By_d$
 $Z_{d+1} X_d + 2By_d Z_{d+1} Z_d s \alpha$ の値が格納されている。 Y_d^W にはステップ 4 1 1
 4 において $Z_{d+1} ((xZ_d + X_d + 2AZ_d)(xX_d + Z_d) - 2AZ_d^2) - X_{d+1}(X_d - xZ_d)^2$ が格
 納され、その後更新が行なわれないので、その値が保持されている。 Z_d^W には
 ステップ 4 1 1 9 において $2By_d Z_{d+1} Z_d s$ が格納され、その後更新が行なわれ
 15 ないので、その値が保持されている。その結果として、ワイエルシュトラス型楕
 円曲線における射影座標 (X_d^W, Y_d^W, Z_d^W) の値が全て復元されている。

上記手順により与えられた $x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$ からワイエルシュ
 トラス型楕円曲線におけるスカラー倍点の射影座標 (X_d^W, Y_d^W, Z_d^W) における
 値が全て復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した
 20 点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、
 数 6 を得る。点 P 及び点 dP はモンゴメリ型楕円曲線上の点であるので、 $By_d^2 =$
 $x_d^3 + Ax_d^2 + x_d$ 及び $By^2 = x^3 + Ax^2 + x$ をみたす。数 6 に代入し、 By_d^2 及び By^2 を
 消去し、式を整理すると、数 6 4 を得る。ここで $x_d = X_d/Z_d$ 、 $x_{d+1} =$
 X_{d+1}/Z_{d+1} であり、この値を代入することにより射影座標の値へと変換する
 25 と、数 6 5 を得る。 $x_d = X_d/Z_d$ であるが、逆元演算の回数を減らす目的で y_d
 の分母と通分することにより、数 6 6 となる。その結果として、

$Y_d' = Z_{d+1} [(X_d + xZ_d + 2AZ_d)(X_d x + Z_d) - 2AZ_d^2] - (X_d - xZ_d)^2 X_{d+1} \cdots$ 数 8 1
 とし、

$$X_d' = 2By_d Z_{d+1} X_d \cdots \text{数 8 2}$$

$$Z_d' = 2ByZ_dZ_{d+1}Z_d \quad \cdots \text{数 } 8 \ 3$$

とすると $(X_d', Y_d', Z_d') = (X_d, Y_d, Z_d)$ となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya,

H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and

5 Their Cryptographic Applications, Public Key Cryptography, LNCS 1751

(2000) pp. 238-257 に記載されている。それによると、変換パラメタを $s\alpha$ とし

て、 $Y_d^W = Y_d'$ 、 $X_d^W = X_d' + \alpha Z_d^W$ 、及び $Z_d^W = sZ_d'$ という関係がある。結果として次の式を得る。

$$Y_d^W = Z_{d+1} [(X_d + xZ_d + 2AZ_d)(X_d x + Z_d) - 2AZ_d^2] - (X_d - xZ_d)^2 X_{d+1} \quad \cdots \text{数 } 8 \ 4$$

$$10 \quad X_d^W = 2ByZ_dZ_{d+1}X_d + \alpha Z_d^W \quad \cdots \text{数 } 8 \ 5$$

$$Z_d^W = 2sByZ_dZ_{d+1}Z_d \quad \cdots \text{数 } 8 \ 6$$

により更新すればよい。ここで、 X_d^W, Y_d^W, Z_d^W は図 4 1 の処理により与えられている。したがって、ワイエルシュトラス型楕円曲線における射影座標

(X_d^W, Y_d^W, Z_d^W) の値が全て復元されていることになる。

- 15 上記手順はステップ 4 1 0 1、ステップ 4 1 0 5、ステップ 4 1 0 6、ステップ 4 1 0 8、ステップ 4 1 1 0、ステップ 4 1 1 1、ステップ 4 1 1 3、ステップ 4 1 1 5、ステップ 4 1 1 6、ステップ 4 1 1 7、ステップ 4 1 1 8、ステップ 4 1 1 9、ステップ 4 1 2 0 及びステップ 4 1 2 1 において有限体上の乗算の計算量を必要とする。また、ステップ 4 1 0 4 において有限体上の 2 乗算の計算
- 20 量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2 乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の 2 乗算の計算量を S とすると、上記手順は $14M + S$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が 160 ビットであれば、高速スカラー倍計算の計算量は
- 25 およそ $1500M$ 弱と見積もられる。 $S = 0.8M$ と仮定すると座標復元の計算量は $14.8M$ であり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた X_d^W, Y_d^W, Z_d^W の値が計算できれば X_d^W, Y_d^W, Z_d^W の値が復元できる。また、ワイエル

シュトラス型楕円曲線においてアフィン座標におけるスカラー倍点 dP を $dP=$

(x_d^W, y_d^W) とすると、 x_d^W, y_d^W が上記計算式により与えられる値を取るよう
に X_d^W, Y_d^W, Z_d^W の値を選択し、その値が計算できれば X_d^W, Y_d^W, Z_d^W が
復元できる。それらの場合においては一般的に復元に必要となる計算量が増大す

- 5 る。また、モンゴメリ型楕円曲線のパラメタである A 乃至は B の値やモンゴメリ型
楕円曲線への変換パラメタ s の値を小さくすることにより、ステップ4106、
ステップ4115乃至はステップ4119における乗算の計算量を削減すること
ができる。

- 次に、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d,$
10 X_{d+1}, Z_{d+1} を出力するアルゴリズムについて説明する。

- 第21実施例の高速スカラー倍計算部202の高速スカラー倍計算方法として、
第9実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値 d 及び
ワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力す
るアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカ
15 ラー倍計算部202において上記アルゴリズムを用いなくても、スカラー値 d 及び
ワイエルシュトラス型楕円曲線上の点 P から、 $X_d, Z_d, X_{d+1}, Z_{d+1}$ を出力す
るアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- スカラー倍計算部103における座標復元部203の座標復元に必要な計算量
は $14M+S$ であり、これは高速スカラー倍計算部202の高速スカラー倍計算
20 に必要な計算量の $(9.2k-3.6)M$ とに比べてはるかに小さい。したがっ
て、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカ
ラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $S=0.8M$
と仮定すると、この計算量はおおよそ $(9.2k+11.2)M$ と見積もること
ができる。例えばスカラー値 d が160ビット($k=160$)であれば、このス
25 カラー倍計算に必要な計算量は1483Mとなる。楕円曲線としてワイエルシュ
トラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした
混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座
標として出力する場合に必要な計算量はおおよそ1600Mであり、これと
比べて必要となる計算量は削減されている。

第22実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部103が、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点 (x_d^W, y_d^W) を計算し出力する。スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P をスカラー倍計算部103に入力すると高速スカラー倍計算部202がそれを受け取る。高速スカラー倍計算部202は受け取ったスカラー値 d と与えられたワイエルシュトラス型楕円曲線上の点 P からモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点 $P = (x, y)$ と共にその情報を座標復元部203に与える。座標復元部203は与えられた座標の値 x_d 、 x_{d+1} 、 x 及び y よりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d^W, y_d^W)$ の座標 y_d^W の復元を行なう。スカラー倍計算部103はワイエルシュトラス型楕円曲線上でアフィン座標において完全に座標が与えられたスカラー倍点 (x_d^W, y_d^W) を計算結果として出力する。

次に図42により、座標 x 、 y 、 x_d 、 x_{d+1} が与えられた場合に、 x_d^W 、 y_d^W を出力する座標復元部の処理について説明する。

座標復元部203では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP = (x_d, y_d)$ の座標のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P = (x_{d+1}, y_{d+1})$ の座標のうち x_{d+1} 、スカラー倍計算部103に入力されたモンゴメリ型楕円曲線上の点 P をアフィン座標で表した (x, y) を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点 (x_d^W, y_d^W) を出力する。

ステップ4201において $x_d \times x$ が計算され、レジスタ T_1 に格納される。ステップ4202において $T_1 + 1$ が計算される。ここでレジスタ T_1 には $x_d x$ が格納されており、したがって $x_d x + 1$ が計算される。その結果がレジスタ T_1 に格納

される。ステップ4 2 0 3において x_d+x が計算され、レジスタ T_2 に格納される。ステップ4 2 0 4において T_2+2A が計算される。ここでレジスタ T_2 には x_d+x が格納されており、したがって x_d+x+2A が計算される。その結果がレジスタ T_2 に格納される。ステップ4 2 0 5において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $x_d x+1$ がレジスタ T_2 には x_d+x+2A がそれぞれ格納されており、したがって $(x_d x+1)(x_d+x+2A)$ が計算される。その結果がレジスタ T_1 に格納される。ステップ4 2 0 6において T_1-2A が計算される。ここでレジスタ T_1 には $(x_d x+1)(x_d+x+2A)$ が格納されており、したがって $(x_d x+1)(x_d+x+2A)-2A$ が計算される。その結果がレジスタ T_1 に格納される。ステップ4 2 0 7において x_d-x が計算され、レジスタ T_2 に格納される。ステップ4 2 0 8において T_2 の2乗が計算される。ここでレジスタ T_2 には x_d-x が格納されており、したがって $(x_d-x)^2$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4 2 0 9において $T_2 \times x_{d+1}$ が計算される。ここでレジスタ T_2 には $(x_d-x)^2$ が格納されており、したがって $(x_d-x)^2 x_{d+1}$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4 2 1 0において T_1-T_2 が計算される。ここでレジスタ T_1 には $(x_d x+1)(x_d+x+2A)-2A$ がレジスタ T_2 には $(x_d-x)^2 x_{d+1}$ がそれぞれ格納されており、したがって $(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$ が計算される。その結果がレジスタ T_1 に格納される。ステップ4 2 1 1において $2B \times y$ が計算され、レジスタ T_2 に格納される。ステップ4 2 1 2において T_2 の逆元が計算される。ここでレジスタ T_2 には $2By$ が格納されており、したがって $1/2By$ が計算される。その結果がレジスタ T_2 に格納される。ステップ4 2 1 3において $T_1 \times T_2$ が計算される。ここでレジスタ T_1 には $(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$ がレジスタ T_2 には $1/2By$ がそれぞれ格納されており、したがって $\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/2By$ が計算される。その結果がレジスタ T_1 に格納される。ステップ4 2 1 4において $T_1 \times (1/s)$ が計算される。ここでレジスタ T_1 には $\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/2By$ が格納されており、したがって $\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/2Bys$ が計算される。その結果がレジスタ y_d^W に格納される。ステップ4 2 1 5において $x_d \times (1/s)$ が計算され、レジスタ T_1 に格納される。ステ

ップ4 2 1 6において $T_1 + \alpha$ が計算される。ここでレジスタ T_1 には x_d/s が格納されており、したがって $(x_d/s) + \alpha$ が計算される。その結果がレジスタ x_d^W に格納される。したがってレジスタ x_d^W には $(x_d/s) + \alpha$ が格納されている。レジスタ y_d^W はステップ4 2 1 4において $\{(x_d x + 1)(x_d + x + 2A) - 2A - (x_d - x)^2$

- 5 $x_{d+1}\}/2Bys$ が格納され、その後更新されないで、その値が保持されている。

上記手順によりスカラー倍点のy座標 y_d が復元される理由は以下の通りである。点 $(d+1)P$ は点 dP に点 P を加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数6を得る。点 P 及び点 dP はモンゴメリ型楕円曲線上の点であるので、 $By_d^2 = x_d^3 + Ax_d^2 + x_d$ 及び $By^2 = x^3 + Ax^2 + x$ をみだす。

- 10 数6に代入し、 By_d^2 及び By^2 を消去し、式を整理すると、数6 4を得る。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp.238-257 に記載されている。それによると、
- 15 変換パラメタを s, α として、 $y_d^W = s^{-1} y_d$ 及び $x_d^W = s^{-1} x_d + \alpha$ の関係がある。結果として数8 7、数6 3を得る。

$$y_d^W = \{(x_d x + 1)(x_d + x + 2A) - 2A - (x_d - x)^2 x_{d+1}\} / (2sBy) \quad \cdots \text{数8 7}$$

ここで、 x_d^W, y_d^W は図4 2により与えられる。したがって、アフィン座標 (x_d^W, y_d^W) の値は全て復元されていることになる。

- 20 上記手順はステップ4 2 0 1、ステップ4 2 0 5、ステップ4 2 0 9、ステップ4 2 1 1、ステップ4 2 1 3、ステップ4 2 1 4及びステップ4 2 1 5において有限体上の乗算の計算量を必要とする。また、ステップ4 2 0 8において有限体上の2乗算の計算量を必要とする。さらにステップ4 2 1 2において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、2乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量を M 、有限体上の2乗算の計算量を S 、有限体上の逆元演算の計算量を I とすると、上記手順は $7M + S + I$ の計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 d が1 6 0ビットであれば、高速スカラー倍計算の計算量は

およそ1500M弱と見積もられる。 $S=0$ 、8M及び $I=40M$ と仮定すると座標復元の計算量は47.8Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

- 尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば y_d^W の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメータであるA乃至はBやモンゴメリ型楕円曲線への変換パラメータsの値を小さくすることにより、ステップ4206、ステップ4211、ステップ4214乃至はステップ4215における乗算の計算量を削減することができる。
- 10 次に図45により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、 x_d 、 x_{d+1} を出力する高速スカラー倍計算部の処理について説明する。高速スカラー倍計算部202では、スカラー倍計算部103に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点 $dP=(x_d, y_d)$ のうち x_d 、アフィン座標で表されたモンゴメリ型楕円曲線上の点 $(d+1)P=(x_{d+1}, y_{d+1})$ のうち x_{d+1} を出力する。ステップ4516として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ4501として、変数Iに初期値1を代入する。ステップ4502として、点Pの2倍点2Pを計算する。ここで
- 15 点Pは射影座標において $(x, y, 1)$ として表し、モンゴメリ型楕円曲線の射影座標における2倍算の公式を用いて2倍点2Pを計算する。ステップ4503として、スカラー倍計算部103に入力された楕円曲線上の点Pとステップ4502で求めた点2Pを、点の組 $(P, 2P)$ として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ4504として、変数Iとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ4515へ行く。一致しなければ
- 20 ステップ4505へ行く。ステップ4505として、変数Iを1増加させる。ステップ4506として、スカラー値のI番目のビットの値が0であるか1であるかを判定する。そのビットの値が0であればステップ4507へ行く。そのビットの値が1であればステップ4510へ行く。ステップ4507として、射影座
- 25

- 標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 4 5 0 8 へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ 4 5 0 8 として、射影座標により表された点の組 $(mP, (m+1)P)$
- 5 から点 mP の 2 倍算 $2(mP)$ を行ない、点 $2mP$ を計算する。その後ステップ 4 5 0 9 へ行く。ここで、2 倍算 $2(mP)$ は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算される。ステップ 4 5 0 9 として、ステップ 4 5 0 8 で求めた点 $2mP$ とステップ 4 5 0 7 で求めた点 $(2m+1)P$ を点の組 $(2mP, (2m+1)P)$ として、点の組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 4 5 0 4 へ戻る。
- 10 ここで、点 $2mP$ 、点 $(2m+1)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ 4 5 1 0 として、射影座標により表された点の組 $(mP, (m+1)P)$ から点 mP と点 $(m+1)P$ の加算 $mP+(m+1)P$ を行ない、点 $(2m+1)P$ を計算する。その後ステップ 4 5 1 1 へ行く。ここで、加算 $mP+(m+1)P$ は、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ 4 5 1 1 として、射影座
- 15 標により表された点の組 $(mP, (m+1)P)$ から点 $(m+1)P$ の 2 倍算 $2((m+1)P)$ を行ない、点 $(2m+2)P$ を計算する。その後ステップ 4 5 1 2 へ行く。ここで、2 倍算 $2((m+1)P)$ は、モンゴメリ型楕円曲線の射影座標における 2 倍算の公式を用いて計算される。ステップ 4 5 1 2 として、ステップ 4 5 1 0 で求めた点 $(2m+1)P$ とステップ 4 5 1 1 で求めた点 $(2m+2)P$ を点の組 $((2m+1)P, (2m+2)P)$ として、点の
- 20 組 $(mP, (m+1)P)$ の代わりに格納する。その後ステップ 4 5 0 4 へ戻る。ここで、点 $(2m+1)P$ 、点 $(2m+2)P$ 、点 mP 及び点 $(m+1)P$ は全て射影座標において表されている。ステップ 4 5 1 5 として、射影座標で表された点 $mP=(X_m, Y_m, Z_m)$ より X_m 及び Z_m をそれぞれ X_d 及び Z_d とし、射影座標で表された点 $(m+1)P=(X_{m+1}, Y_{m+1}, Z_{m+1})$ より X_{m+1} 及び Z_{m+1} をそれぞれ X_{d+1} 及び Z_{d+1} とする。ここで、 Y_m
- 25 及び Y_{m+1} は、モンゴメリ型楕円曲線の射影座標における加算公式及び 2 倍算の公式では Y 座標を求める事ができないので、求まっていない。 $X_d, Z_d, X_{d+1}, Z_{d+1}$ より、 $x_d=X_d Z_{d+1}/Z_d Z_{d+1}$, $x_{d+1}=Z_d X_{d+1}/Z_d Z_{d+1}$ として x_d, x_{d+1} を求める。その後ステップ 4 5 1 3 へ行く。ステップ 4 5 1 3 として、 x_d, x_{d+1} を出力する。上記手順により、 m とスカラー値 d はビット長が等しく

さらにそのビットのパターンも同じとなる為、等しくなる。

- モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、 $Z_1=1$ ととることにより $3M+2S$ となる。ここで M は有限体上の乗算の計算量、 S は有限体上の2乗算の計算量である。モンゴメリ型楕円曲線の射影座標における2倍算の
- 5 公式の計算量は、 $3M+2S$ である。スカラー値の I 番目のビットの値が0であれば、ステップ4507において加算の計算量、ステップ4508において2倍算の計算量が必要となる。すなわち $6M+4S$ の計算量が必要となる。スカラー値の I 番目のビットの値が1であれば、ステップ4510において加算の計算量、ステップ4511において2倍算の計算量が必要となる。すなわち $6M+4S$ の
- 10 計算量が必要である。いずれの場合においても $6M+4S$ の計算量が必要である。ステップ4504、ステップ4505、ステップ4506、ステップ4507、ステップ4508、ステップ4509乃至はステップ4504、ステップ4505、ステップ4506、ステップ4510、ステップ4511、ステップ4512の繰り返しの回数は、(スカラー値 d のビット長) - 1 回となるので、ステップ4502での2倍算の計算量及びステップ4515でのアフィン座標への変換の計算量を考慮に入れると、全体の計算量は $(6M+4S)k + 3M - 2S + I$ となる。ここで k はスカラー値 d のビット長である。一般的には、計算量 S は、 $S=0.8M$ 程度、計算量 I は $I=40M$ 程度と見積もられるので、全体の計算量はおよそ $(9.2k + 41.4)M$ となる。例えばスカラー値 d が160ビット
- 20 ット ($k=160$) であれば、上記手順のアルゴリズムの計算量はおよそ $1513M$ となる。スカラー値 d のビットあたりの計算量としてはおよそ $9.2M$ となる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp.51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおよそ $10M$ と見積もられ、これ以外にアフィン座標への変換の計算量が必要となる。例えばスカラー値 d が160ビット ($k=160$) であれば、このスカラー倍計算方法の計算
- 25

量はおおよそ1640Mとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部202において上記手順のアルゴリズムを用いなくとも、スカラー値 d 及びワイエルシュトラス型楕円曲線上の点 P から、 x_d ,

- 5 x_{d+1} を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いてもよい。

- スカラー倍計算部103における座標復元部203の座標復元に必要な計算量は $7M + S + I$ であり、これは高速スカラー倍計算部202の高速スカラー倍計算に必要な計算量の $(9.2k + 41.4)M$ とに比べてはるかに小さい。したがって、スカラー倍計算部103のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。 $I = 40M$ 、 $S = 0.8M$ と仮定すると、この計算量はおおよそ $(9.2k + 89.2)M$ と見積もることができる。例えばスカラー値 d が160ビット($k = 160$)であれば、このスカラー倍計算に必要な計算量は1561Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要な計算量はおおよそ1640Mであり、これと比べて必要となる計算量は削減されている。
- 10
15

- 以上、図1に示した暗号／復号処理装置を復号化処理を行う装置として第1から第22の実施例を説明したが、同様に暗号化処理を行う装置としても利用できる。その場合には、既に説明したように暗号／復号処理装置のスカラー倍計算部103は、既に説明した楕円曲線上の点 Q 、乱数 k によるスカラー倍点と、公開鍵 aQ と乱数 k によるスカラー倍点を出力する。このとき、実施例1から22で説明したスカラー値 d を乱数 k 、楕円曲線上の点 P を楕円曲線上の点 Q 、公開鍵 aQ として同様の処理を行うことにより、それぞれのスカラー倍点を求めることができる。
- 20
25

尚、図1に示した暗号／復号処理装置は、暗号化、復号化の両方を行えるように示したが、暗号化の処理のみ、あるいは復号化の処理のみを行えるように構成してもよい。

また、第1から第22の実施例で説明した処理については、コンピュータ読み取り可能な記憶媒体に格納されたプログラムであってもよい。この場合は、そのプログラムを図1の記憶部へ読み込み、処理部であるCPUなどの演算装置がこのプログラムに従って、処理を行う。

- 5 図27は、図1の暗号処理システムにおける秘密情報を用いた暗号処理において、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法の実施例を示す図である。図33は、図27のスカラー倍計算方法の実施例における処理の流れを示すフローチャートである。

- 図33において、図27のスカラー倍計算部2701は以下のようにして、ス
- 10 カラー値及びワイエルシュトラス型楕円曲線上の点から、ワイエルシュトラス型楕円曲線上で完全な座標が与えられたスカラー倍点を計算し出力する。スカラー値及びワイエルシュトラス型楕円曲線上の点をスカラー倍計算部2701に入力すると、楕円曲線変換部2704がワイエルシュトラス型楕円曲線上の点をモンゴメリ型楕円曲線上の点に変換する。(ステップ3301)。高速スカラー倍計
- 15 算部2702はスカラー倍計算部2701に入力されたスカラー値及び楕円曲線変換部2704が変換したモンゴメリ型楕円曲線上の点を受け取る(ステップ3302)。高速スカラー倍計算部2702は受け取ったスカラー値とモンゴメリ型楕円曲線上の点からモンゴメリ型楕円曲線上のスカラー倍点の座標の一部の値を計算し(ステップ3303)、その情報を座標復元部2703に与える(ステ
- 20 ップ3304)。座標復元部2703は与えられたモンゴメリ型楕円曲線上のスカラー倍点の情報及び楕円曲線変換部2704により変換されたモンゴメリ型楕円曲線上の点よりモンゴメリ型楕円曲線上のスカラー倍点の座標の復元を行なう(ステップ3305)。楕円曲線逆変換部2705は、座標復元部2703により復元されたモンゴメリ型楕円曲線上のスカラー倍点をワイエルシュトラス型楕
- 25 円曲線上のスカラー倍点に変換する(ステップ3306)。スカラー倍計算部2701はワイエルシュトラス型楕円曲線上で完全に座標が与えられたスカラー倍点を計算結果として出力する。(ステップ3307)。

スカラー倍計算部2701における高速スカラー倍計算部2702及び座標復元部2703が実行するモンゴメリ型楕円曲線上のスカラー倍計算は、上述した

第1～第5及び第14～第16実施例で説明したモンゴメリ型楕円曲線上におけるスカラー倍計算方法がそのまま適応される。したがってこのスカラー倍計算は、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法である。

図22は、図1の本実施形態の暗号処理システムを署名作成装置として利用する場合の構成を示す。図1の暗号処理部102は、図22の署名作成装置2201では署名部2202になる。図28は、図22の署名作成装置における処理の流れを示すフローチャートである。図29は、図22の署名作成装置における処理の流れを示すシーケンス図である。

図28において、署名作成装置2201は以下のようにして、与えられたメッセージ2205から署名が付随しているメッセージ2206を出力する。メッセージ2205を署名作成装置2201に入力すると署名部2202がそれを受け取る（ステップ2801）。署名部2202はスカラー倍計算部2203に受け取ったメッセージ2205に応じて楕円曲線上の点を与える（ステップ2802）。スカラー倍計算部2203は秘密情報格納部2204より秘密情報であるスカラー値を受け取る（ステップ2803）。スカラー倍計算部2203は受け取った楕円曲線上の点とスカラー値よりスカラー倍点を計算し（ステップ2804）、そのスカラー倍点を署名部2202に送る（ステップ2805）。署名部2202はスカラー倍計算部2203より受け取ったスカラー倍点をもとにして署名作成処理を行なう（ステップ2806）。その結果を署名が付随したメッセージ2206として出力する（ステップ2807）。

上記処理手順を図29のシーケンス図を用いて説明する。まず、署名部2901（図22の2202）の実行する処理について説明する。署名部2901は、入力メッセージを受け取る。署名部2901は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部2902に楕円曲線上の点を与え、そしてスカラー倍計算部2902からスカラー倍点を受け取る。署名部2901は、受け取ったスカラー倍点を用いて署名作成処理を行ない、その結果を出力メッセージとして出力する。

次にスカラー倍計算部2902（図22の2203）の実行する処理について説明する。スカラー倍計算部2902は、署名部2901より楕円曲線上の点を

受け取る。スカラー倍計算部 2902 は、秘密情報格納部 2903 よりスカラー値を受け取る。スカラー倍計算部 2902 は、受け取った楕円曲線上の点及びスカラー値から、完全な座標を与え且つ高速なスカラー倍計算方法により、スカラー倍点を計算し、署名部 2901 にスカラー倍点を送る。

- 5 最後に秘密情報格納部 2903（図 22 の 2204）の実行する処理について説明する。秘密情報格納部 2903 は、スカラー倍計算部 2902 がスカラー倍を計算できるように、スカラー値をスカラー倍計算部 2902 に送る。

- スカラー倍計算部 2203 が実行するスカラー倍計算は、上述した第 1 ～ 第 2 実施例で説明したものがそのまま適応される。したがってこのスカラー倍計算
- 10 は、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法である。そのため署名部 2202 において、署名作成処理を行なう際に、スカラー倍点の完全な座標を用いることができ、その上高速に実行できる。

- 図 23 は、図 1 の本実施形態の暗号処理システムを復号化装置として利用する場合の構成を示す。図 1 の暗号処理部 102 は、図 23 の復号化装置 2301 で
- 15 は復号部 2302 になる。図 30 は、図 23 の復号化装置における処理の流れを示すフローチャートである。図 31 は、図 23 の復号化装置における処理の流れを示すシーケンス図である。

- 図 30 において、復号装置 2301 は以下のようにして、与えられたメッセージ 2305 から復号化されたメッセージ 2306 を出力する。メッセージ 230
- 20 5 を復号装置 2301 に入力すると復号部 2302 がそれを受け取る（ステップ 3001）。復号部 2302 はスカラー倍計算部 2303 に受け取ったメッセージ 2305 に応じて楕円曲線上の点を与える（ステップ 3002）。スカラー倍計算部 2303 は秘密情報格納部 2304 より秘密情報であるスカラー値を受け取る（ステップ 3003）。スカラー倍計算部 2303 は受け取った楕円曲線上
- 25 の点とスカラー値よりスカラー倍点を計算し（ステップ 3004）、そのスカラー倍点を復号部 2302 に送る（ステップ 3005）。復号部 2302 はスカラー倍計算部 2303 より受け取ったスカラー倍点をもとにして復号化処理を行なう（ステップ 3006）。その結果を復号化されたメッセージ 2306 として出力する（ステップ 3007）。

上記処理手順を図31のシーケンス図を用いて説明する。まず、復号化部3101（図23の2302）の実行する処理について説明する。復号化部3101は、入力メッセージを受け取る。復号化部3101は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部3102に楕円曲線上の点を与え、そしてスカラー倍計算部3102からスカラー倍点を受け取る。復号化部3101は、受け取ったスカラー倍点を用いて復号化処理を行ない、その結果を出力メッセージとして出力する。

次にスカラー倍計算部3102（図23の2303）の実行する処理について説明する。スカラー倍計算部3102は、復号化部3101より楕円曲線上の点を受け取る。スカラー倍計算部3102は、秘密情報格納部3103よりスカラー値を受け取る。スカラー倍計算部3102は、受け取った楕円曲線上の点及びスカラー値から、完全な座標を与え且つ高速なスカラー倍計算方法により、スカラー倍点を計算し、復号化部3101にスカラー倍点を送る。

最後に秘密情報格納部3103（図23の2304）の実行する処理について説明する。秘密情報格納部3103は、スカラー倍計算部3102がスカラー倍を計算できるように、スカラー値をスカラー倍計算部3102に送る。

スカラー倍計算部2303が実行するスカラー倍計算は、上述した第1～第2実施例で説明したものがそのまま適応される。したがってこのスカラー倍計算は、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法である。そのため復号部2302において、復号化処理を行なう際に、スカラー倍点の完全な座標を用いることができ、その上高速に実行できる。

以上述べたように本発明によれば、暗号処理システムにおける秘密情報を用いた暗号処理において用いられるスカラー倍計算が高速化されており、暗号処理の高速化が計れる。また、スカラー倍点の座標を完全に与えることができるので、全ての暗号処理を行なうことができる。

請 求 の 範 囲

1. 楕円曲線暗号における標数 5 以上の有限体上定義された楕円曲線において、
スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法
5 であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分
情報から完全な座標を復元するステップとを有するスカラー倍計算方法。

2. 楕円曲線暗号における標数 5 以上の有限体上定義された楕円曲線において、
スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法
10 であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分
情報からアフィン座標において完全な座標を復元するステップとを有するスカ
ラー倍計算方法。

3. 楕円曲線暗号における標数 5 以上の有限体上定義された楕円曲線において、
15 スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法
であって、 前記スカラー倍点の部分情報を計算するステップと、前記スカ
ラー倍点の部分情報から射影座標において完全な座標を復元するステップとを有する
スカラー倍計算方法。

4. 楕円曲線暗号における標数 5 以上の有限体上定義されたモンゴメリ型楕円
20 曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を
計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分
情報から完全な座標を復元するステップとを有するスカラー倍計算方法。

5. 楕円曲線暗号における標数 5 以上の有限体上定義されたワイエルシュトラス
25 ス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点か
らスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分
情報から完全な座標を復元するステップとを有するスカラー倍計算方法。

6. 楕円曲線暗号における標数 5 以上の有限体上定義されたモンゴメリ型楕円

曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

7. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

10 前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

15 8. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

9. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標における

X座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

10. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

- 前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点のx座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点のアフィン座標におけるx座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点のアフィン座標におけるx座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

11. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

- 前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

12. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

- 25 前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、射影

座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

13. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

- 5 前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点の x 座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点のアフィン座標における x 座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点のアフィン座標における x 座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

14. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

- 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からワイエルシュトラス型楕円曲線において完全な座標を復元するステップとを有するスカラー倍計算方法。
- 15

15. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、
- 20

- 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からモンゴメリ型楕円曲線において完全な座標を復元するステップと、前記モンゴメリ型楕円曲線において完全な座標が復元されたスカラー倍点からワイエルシュトラス型楕円曲線におけるスカラー倍点を計算するステップとを有するスカラー倍計算方法。
- 25

16. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点か

らスカラー倍点を計算するスカラー倍計算方法であって、

- 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴ
- 5 メリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有するスカラー倍計算方法。

17. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、
- 10 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴ

- 15 メリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有するスカラー倍計算方法。

18. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、
- 20 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴ

- 25 メリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有する

スカラー倍計算方法。

19. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

- 5 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標、
10 前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有するスカラー倍計算方法。

20. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

- 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴ
20 メリ型楕円曲線においてアフィン座標で与えられたスカラー倍点のx座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点のアフィン座標におけるx座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点のアフィン座標におけるx座標を与え、ワイエルシュトラス型楕円曲線においてア
フィン座標における完全な座標を復元するステップとを有するスカラー倍計算方
25 法。

21. 第1のデータから第2のデータを生成するデータ生成方法であって、請求項1から20の何れか一つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とするデータ生成方法。

22. データから署名データを生成する署名生成方法であって、請求項1から2

0の何れか一つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする署名生成方法。

23. 暗号化されたデータから復号化されたデータを生成する復号化方法であって、請求項1から20の何れか一つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする復号化方法。

24. 楕円曲線暗号における標数5以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算部であって、

- 前記スカラー倍点の部分情報を計算する高速スカラー倍計算部と、前記スカラー倍点の部分情報から完全な座標を復元する座標復元部とを有し、

前記スカラー倍計算部は、高速スカラー倍計算部により前記スカラー倍点の部分情報を計算した後、座標復元部により前記スカラー倍点の部分情報から完全な座標を復元し、スカラー倍点を計算することを特徴とする。

25. 楕円曲線暗号における標数5以上の有限体上定義された楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算部であって、

- 前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換する楕円曲線変換部と、前記スカラー倍点の部分情報を計算する高速スカラー倍計算部と、前記スカラー倍点の部分情報から完全な座標を復元する座標復元部と、モンゴメリ型楕円曲線をワイエルシュトラス型楕円曲線に変換する楕円曲線逆変換部とを有し、

- 前記スカラー倍計算部は、楕円曲線変換部により前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換し、高速スカラー倍計算部によりモンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算し、座標復元部により前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からモンゴメリ型楕円曲線において完全な座標を復元し、楕円曲線逆変換部によりモンゴメリ型楕円曲線において完全な座標が復元されたスカラー倍点からワイエルシュトラス型楕円曲線におけるスカラー倍点を計算し、スカラー倍点を計算することを特徴とする。

26. 請求項1から20の何れか一つに記載のスカラー倍計算方法に係るプログ

ラムを格納したことを特徴とする記憶媒体。

27. 楕円曲線暗号における標数 5 以上の有限体上定義された楕円曲線において、不完全な座標で与えられた楕円曲線上の点から完全な座標を復元する座標復元方法であって、

- 5 前記不完全な座標を持つ点及び前記不完全な座標を持つ点と完全な座標を持つ点との加算及び減算によって得られる点により、前記不完全な座標を持つ点の座標を計算するステップを有する座標復元方法。

28. 楕円曲線暗号における標数 5 以上の有限体上定義された楕円曲線において、不完全な座標で与えられた楕円曲線上の点から完全な座標を復元する座標復元方法であって、

10

前記不完全な座標を持つ点及び前記不完全な座標を持つ点と完全な座標を持つ点との加算によって得られる点から、前記不完全な座標を持つ点と完全な座標を持つ点との減算によって得られる点を計算するステップと、前記不完全な座標を持つ点の座標を計算するステップを有する座標復元方法。

- 15 29. 楕円曲線暗号における標数 5 以上の有限体上定義されたモンゴメリ型楕円曲線において、不完全な座標で与えられたモンゴメリ型楕円曲線上の点からワイエルシュトラス型楕円曲線において完全な座標を復元する座標復元方法であって、

前記モンゴメリ型楕円曲線において不完全な座標を持つ点及び前記モンゴメリ型楕円曲線において不完全な座標を持つ点と完全な座標を持つ点との加算及び減算によって得られる点から、前記モンゴメリ型楕円曲線において不完全な座標を持つ点の座標を計算するステップと、前記完全な座標が計算されたモンゴメリ型楕円曲線の点をワイエルシュトラス型楕円曲線の点に変換するステップとを有する座標復元方法。

- 20 30. 楕円曲線暗号における標数 5 以上の有限体上定義されたモンゴメリ型楕円曲線において、不完全な座標で与えられたモンゴメリ型楕円曲線上の点からワイエルシュトラス型楕円曲線において完全な座標を復元する座標復元方法であって、

前記モンゴメリ型楕円曲線において不完全な座標を持つ点及び前記モンゴメリ型楕円曲線において不完全な座標を持つ点と完全な座標を持つ点との加算によって得られる点から、前記モンゴメリ型楕円曲線において不完全な座標を持つ点と

完全な座標を持つ点との減算によって得られる点を計算するステップと、前記モンゴメリ型楕円曲線において不完全な座標を持つ点の座標を計算するステップと、前記完全な座標が計算されたモンゴメリ型楕円曲線の点をワイエルシュトラス型楕円曲線の点に変換するステップとを有する座標復元方法。



FIG. 1

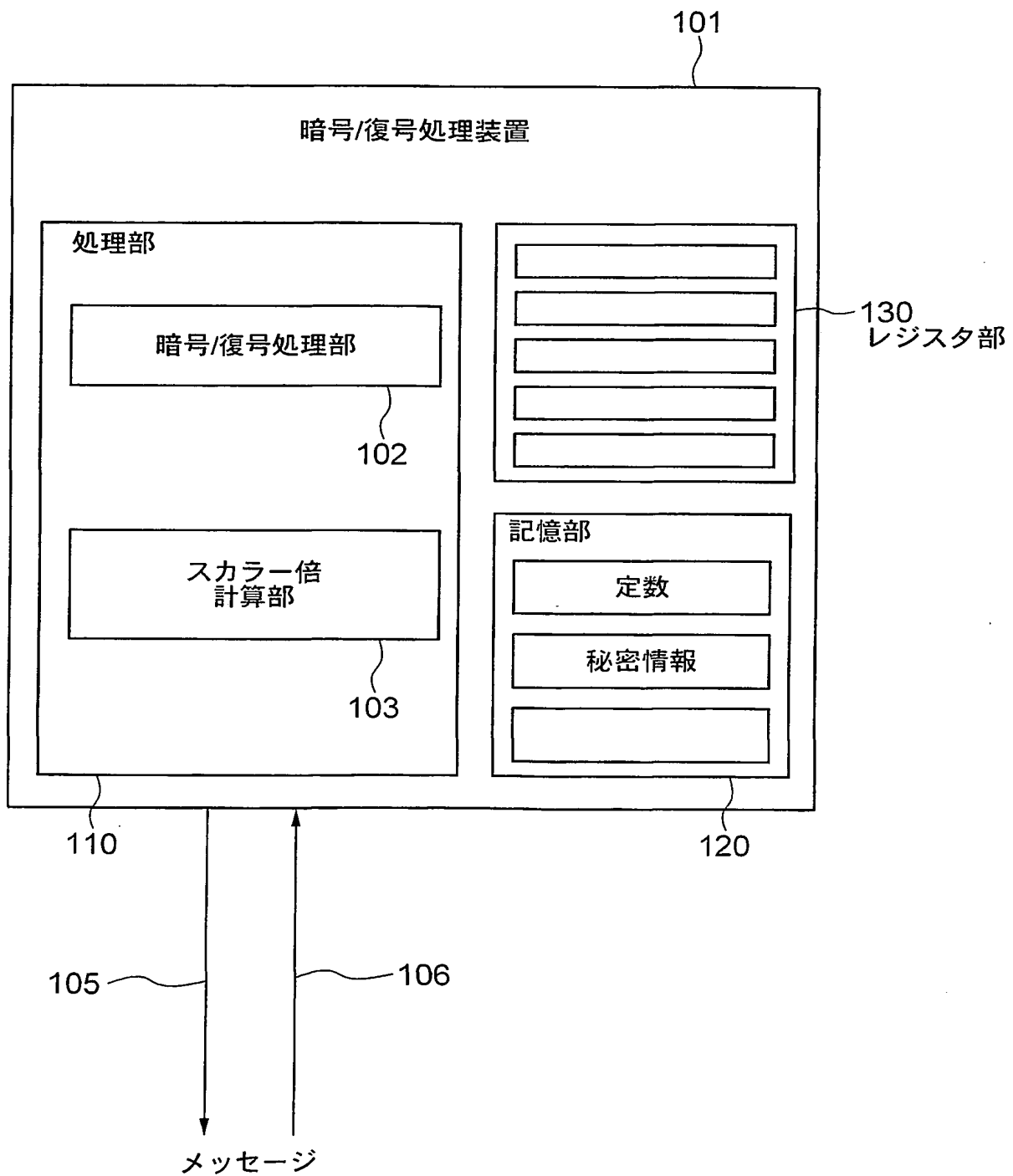




FIG. 2

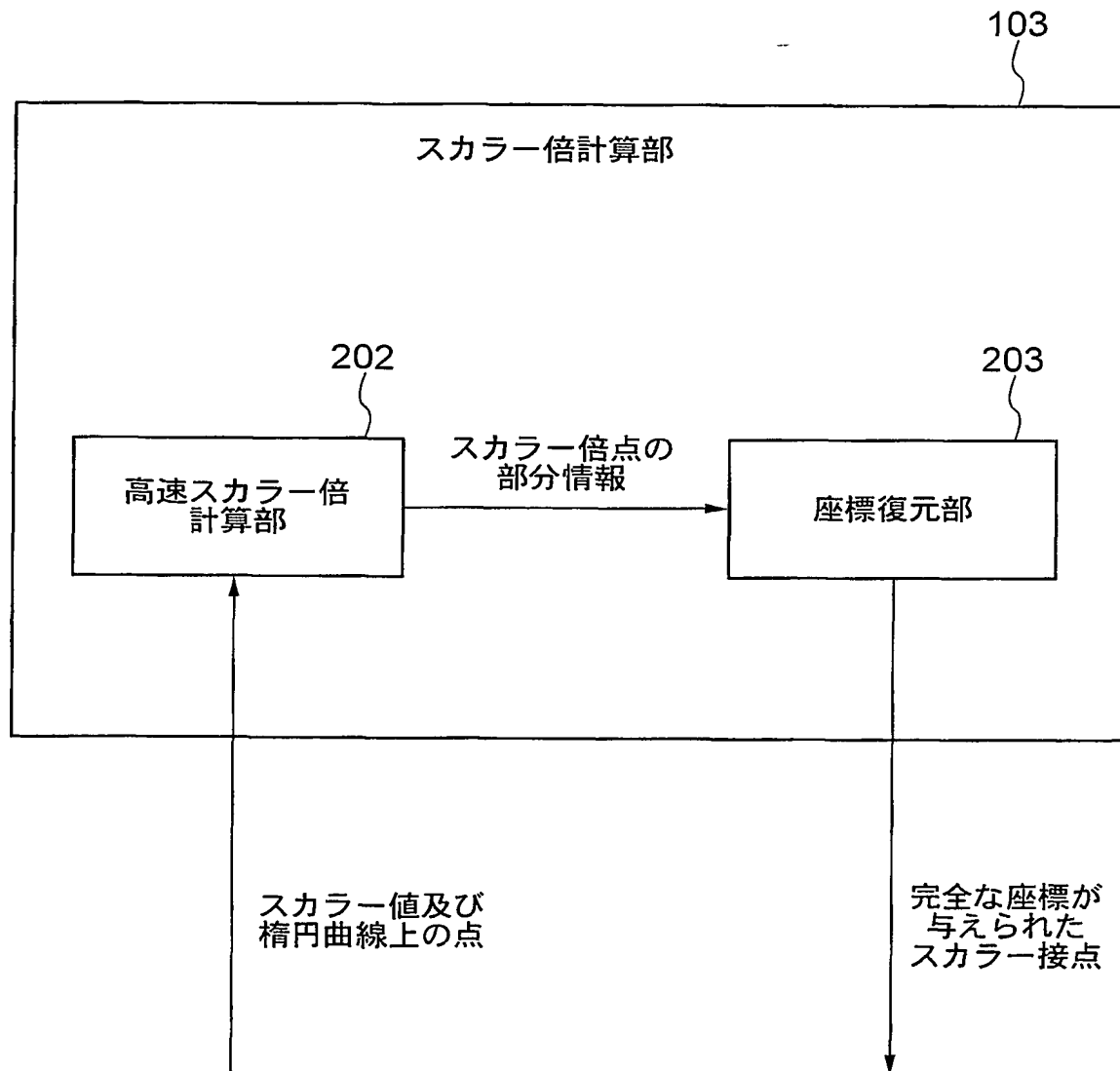
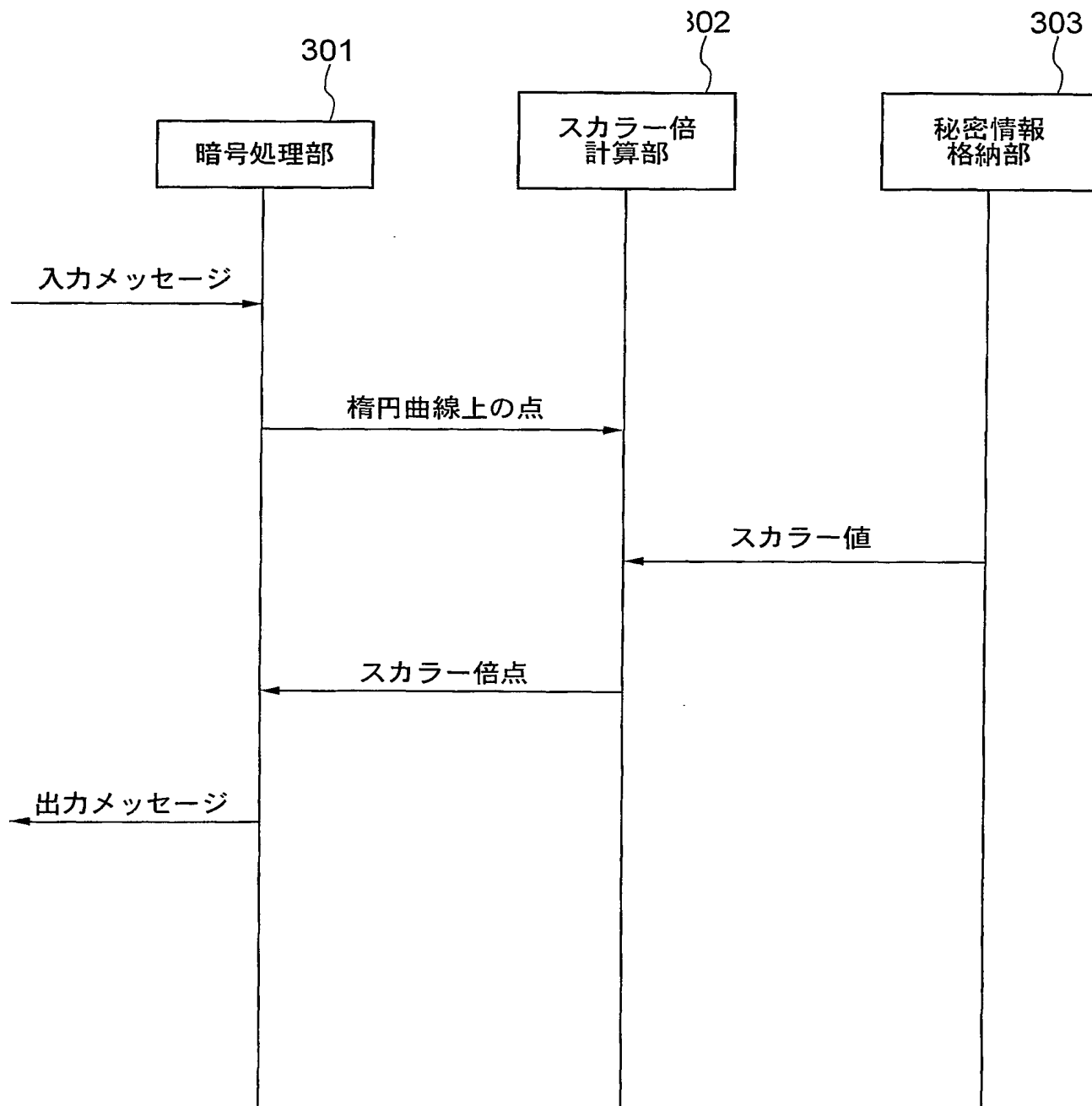




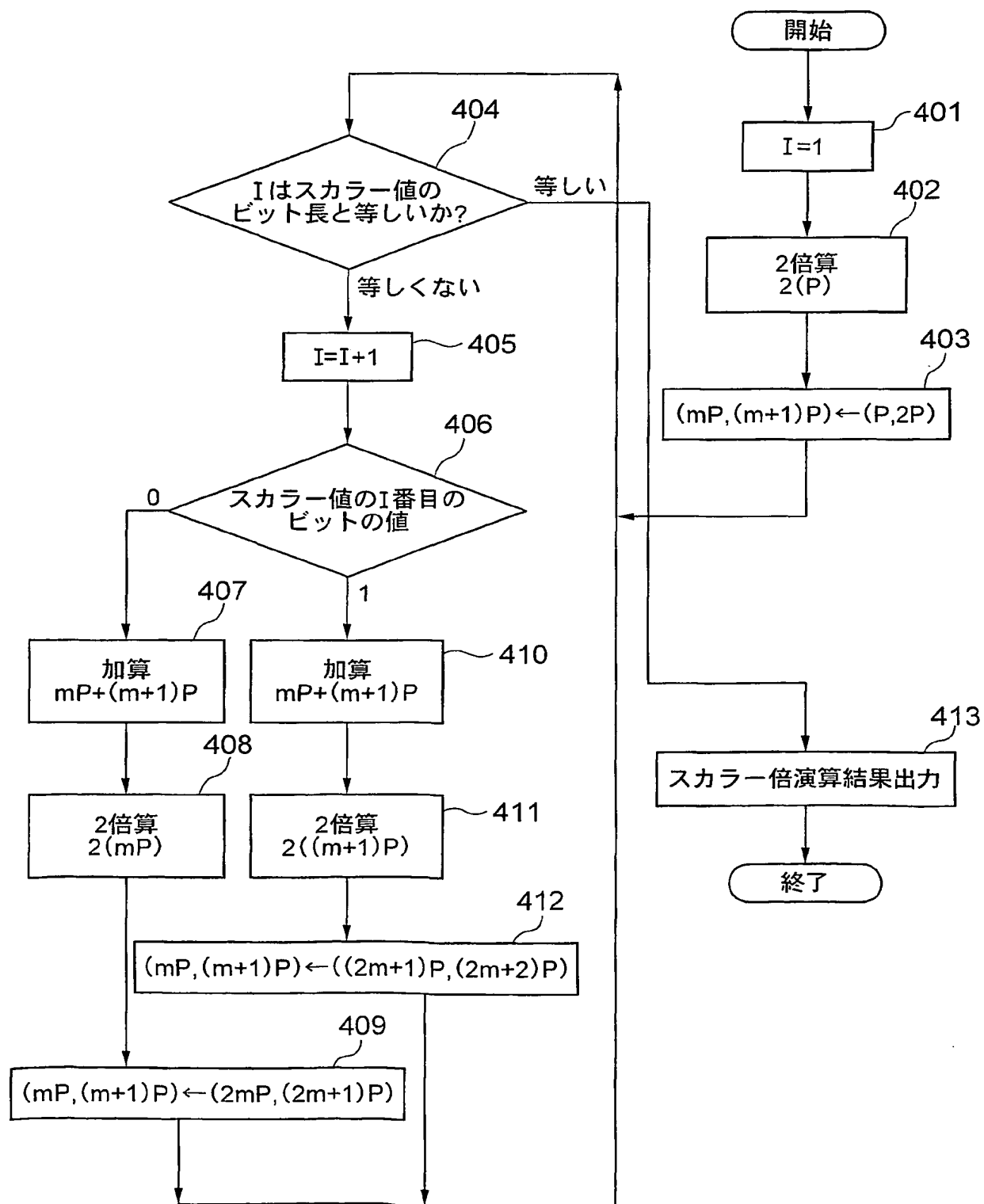
FIG. 3





4/45

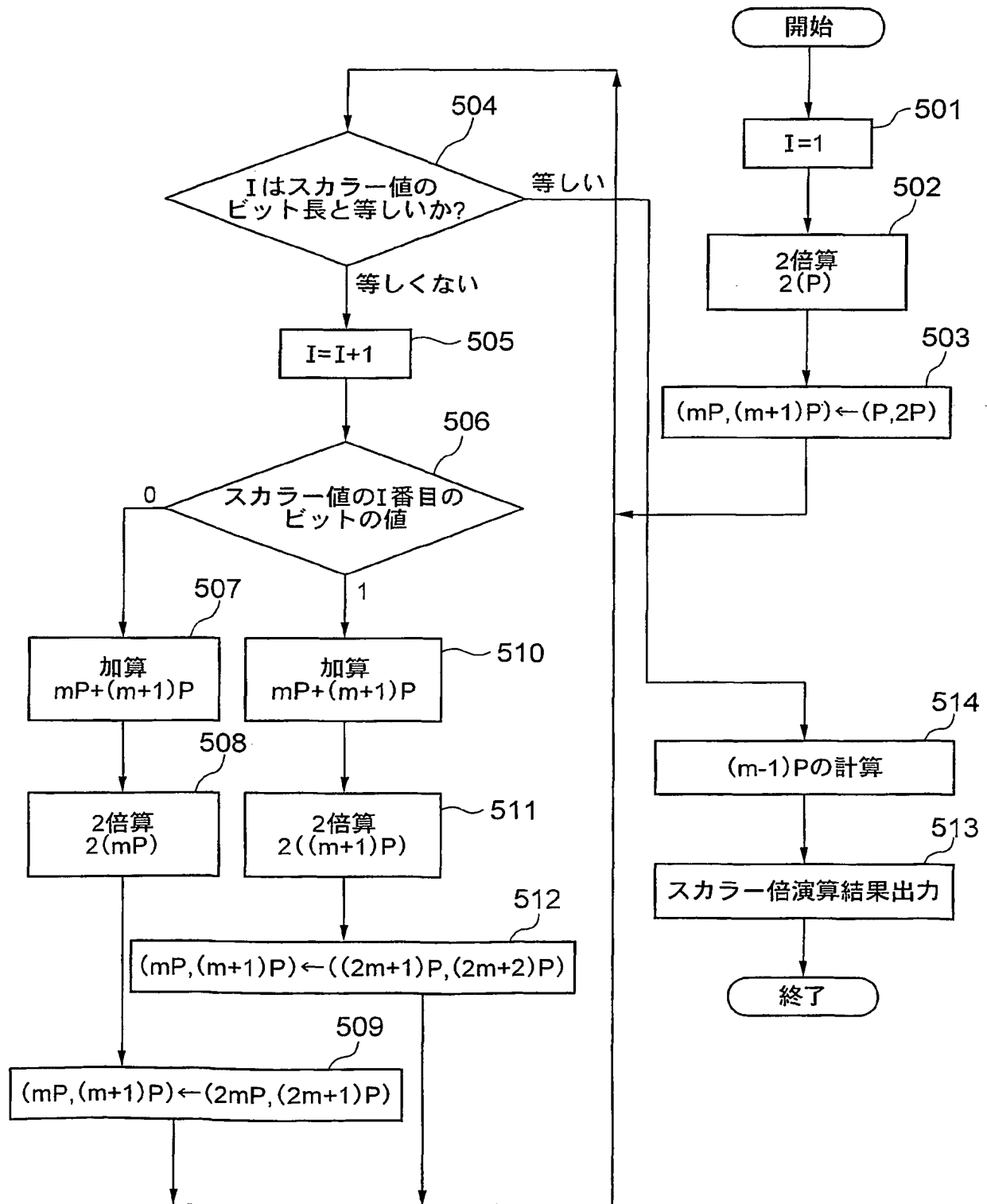
FIG. 4





5/45

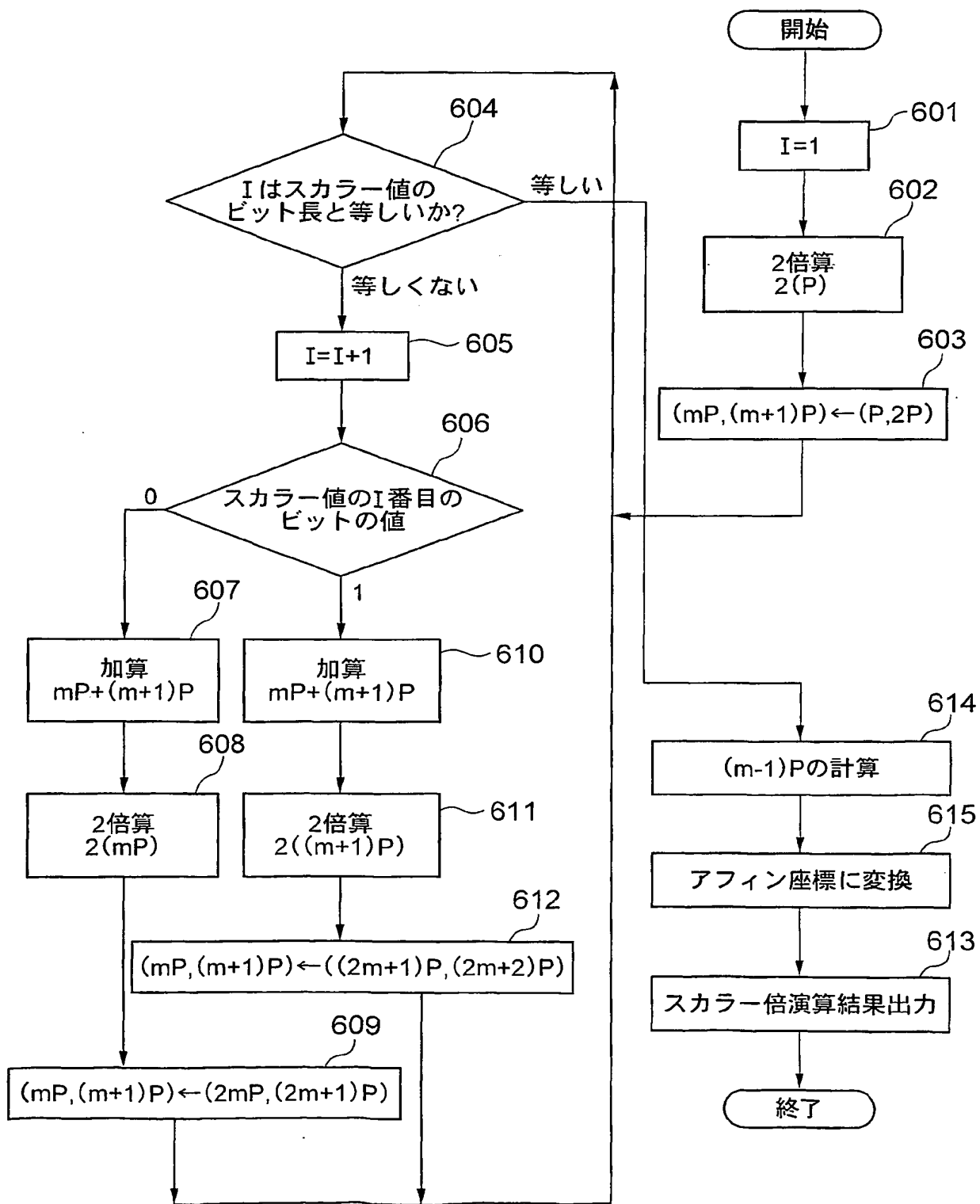
FIG. 5





6/45

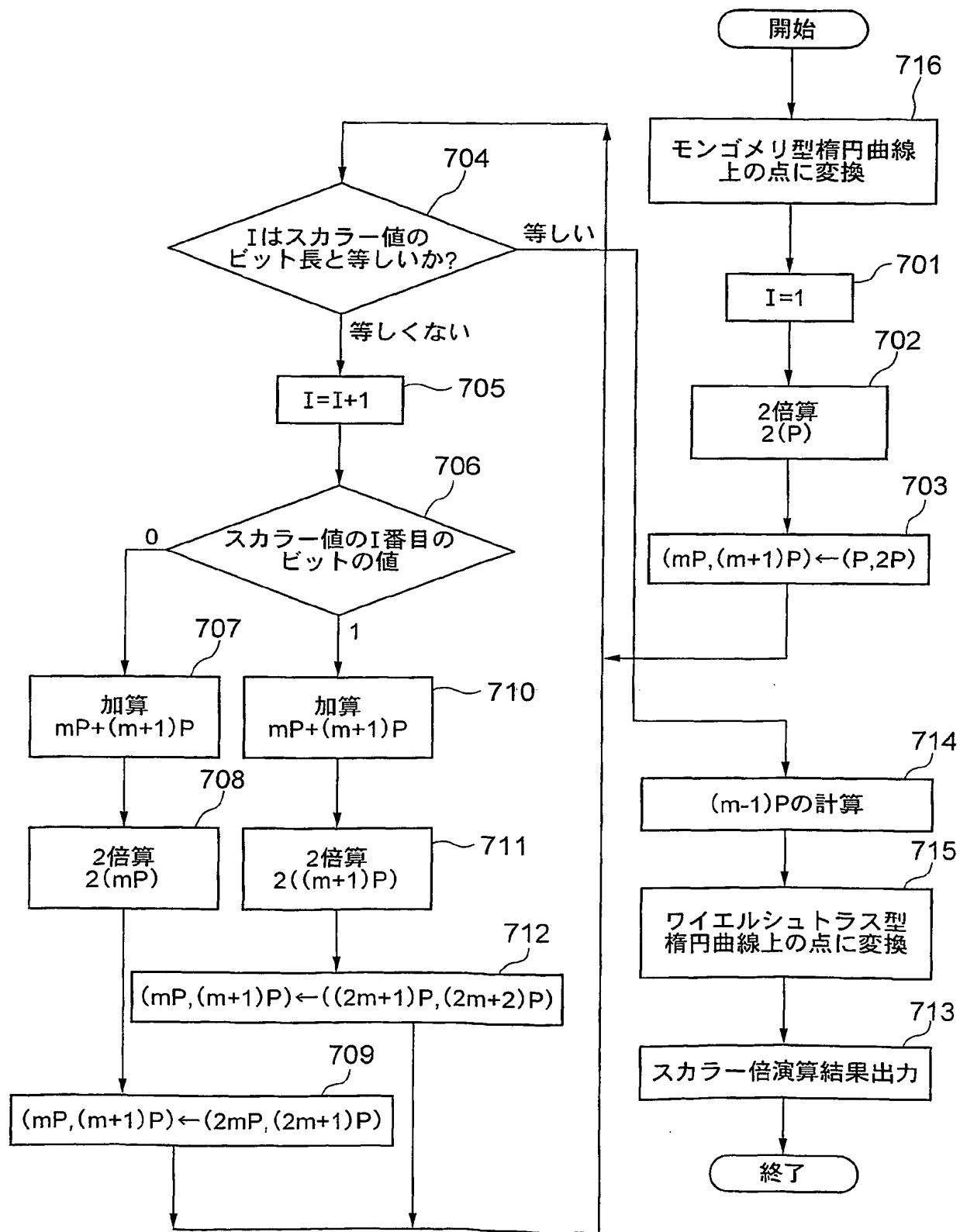
FIG. 6





7/45

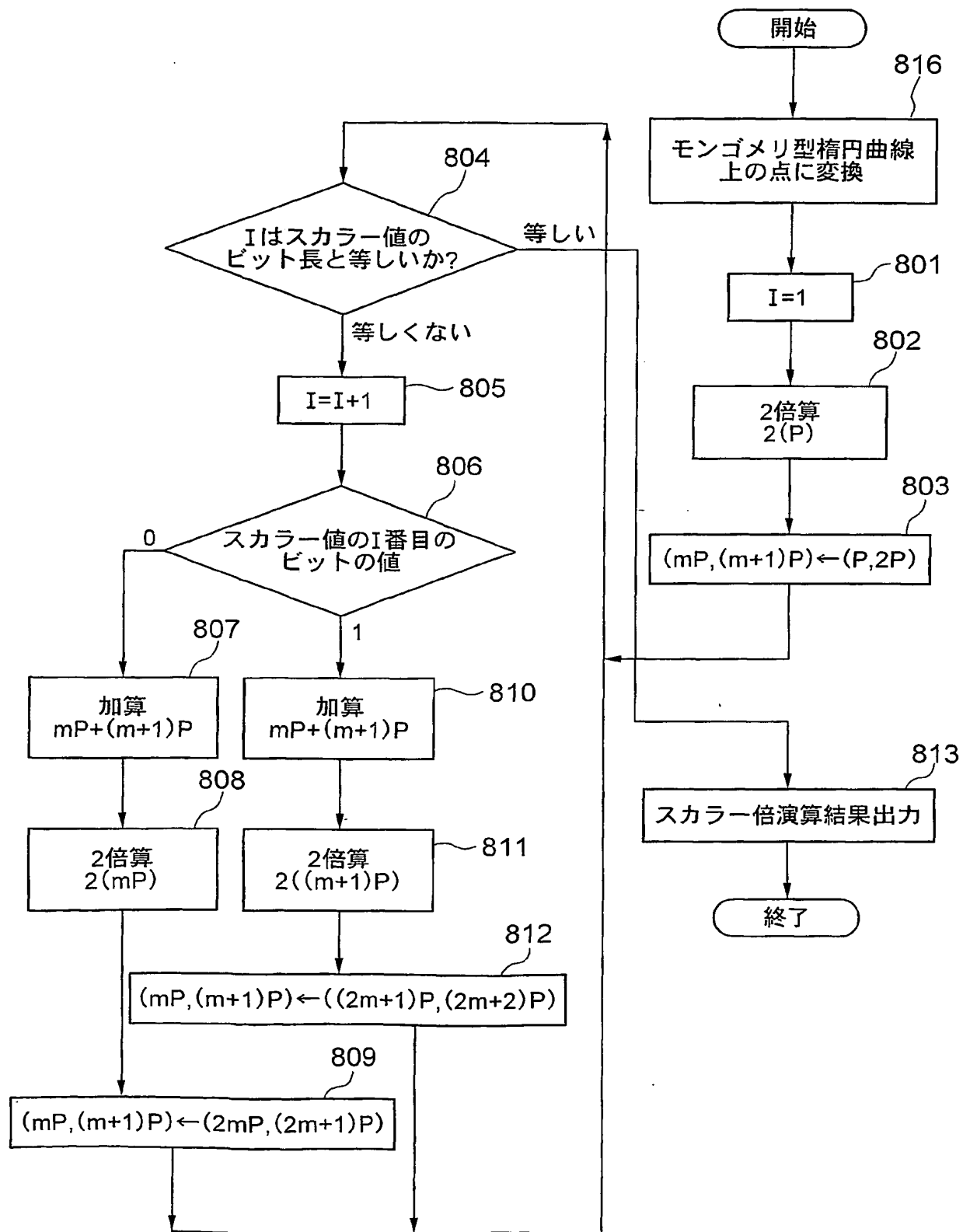
FIG. 7





8/45

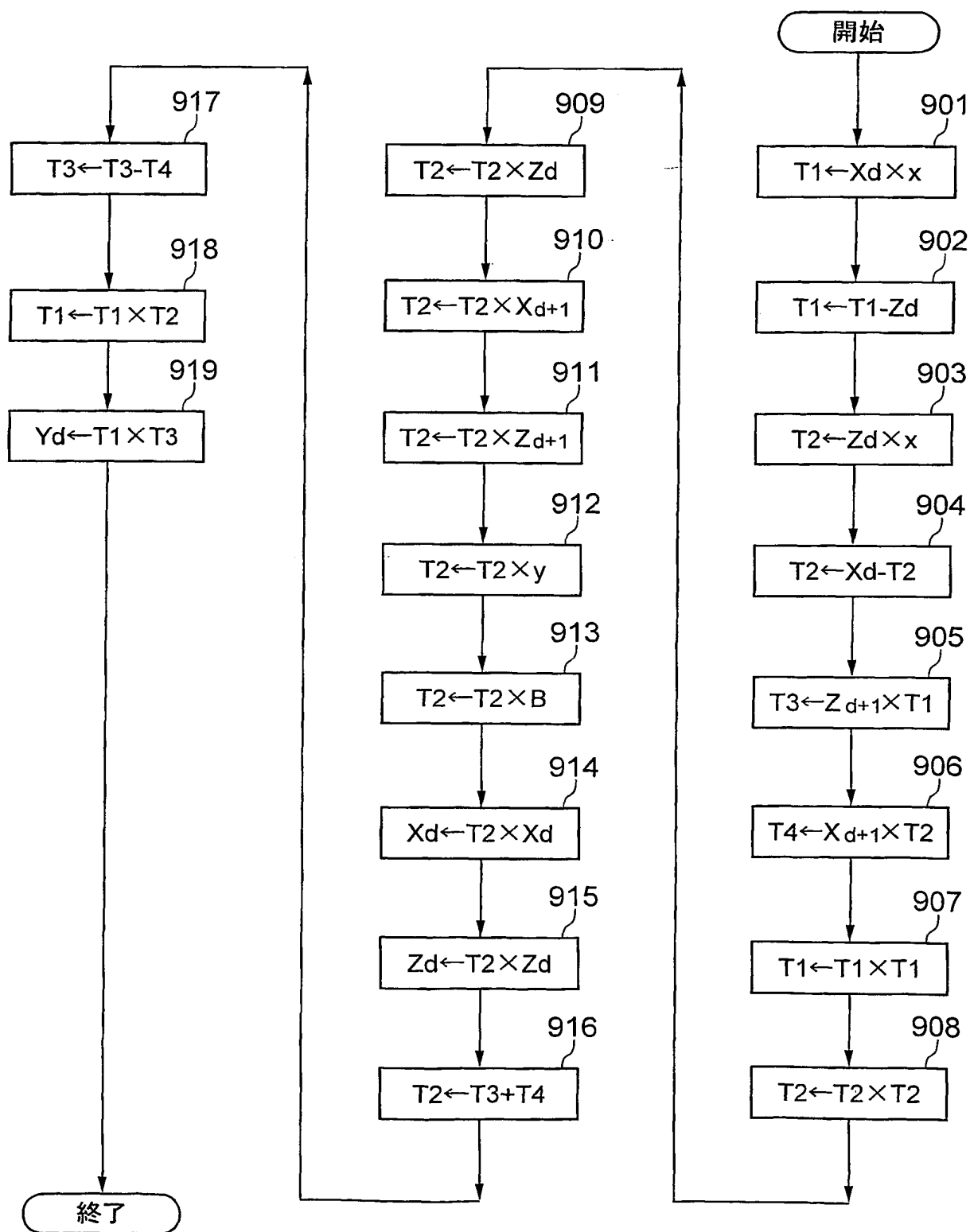
FIG. 8





9/45

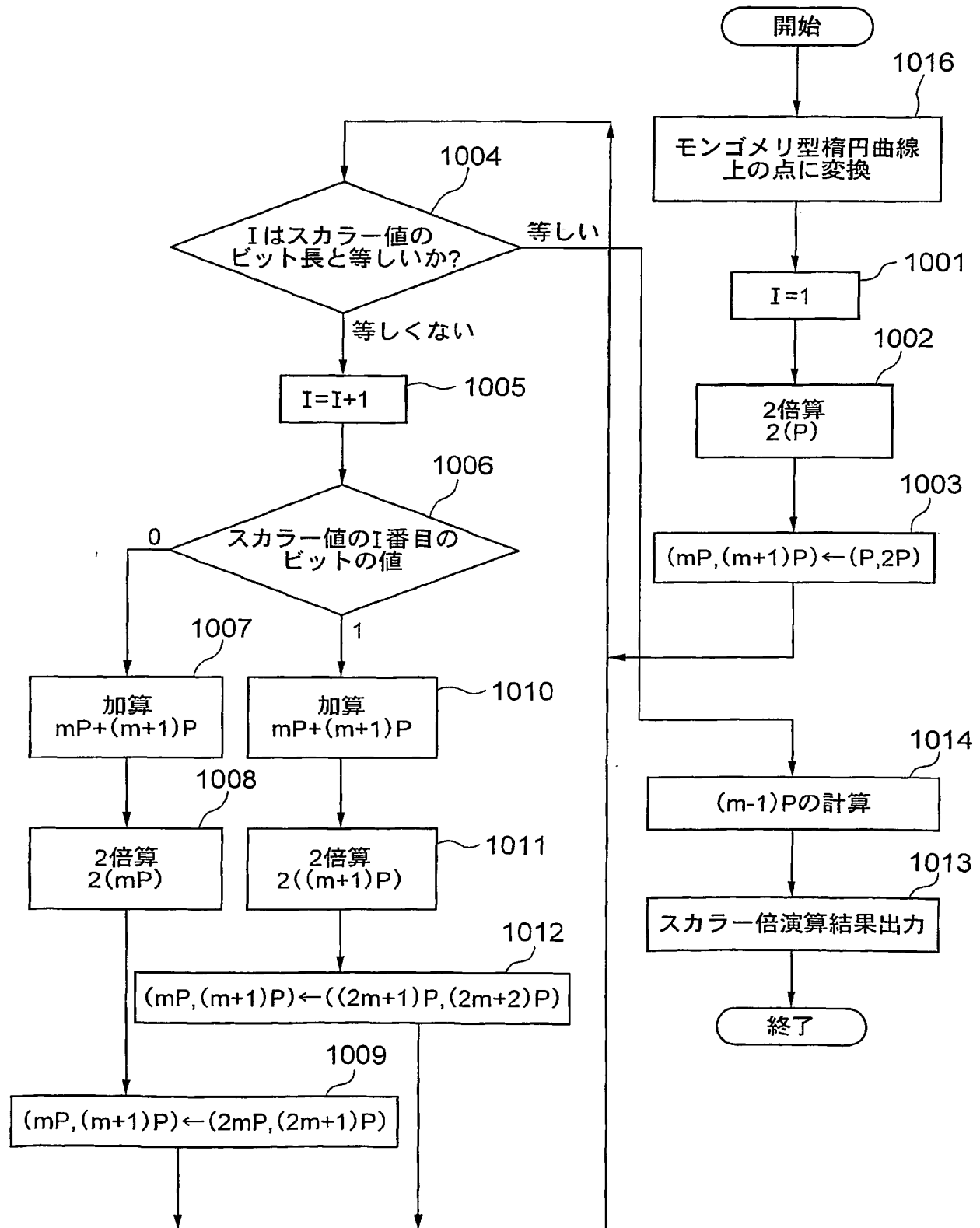
FIG. 9





10/45

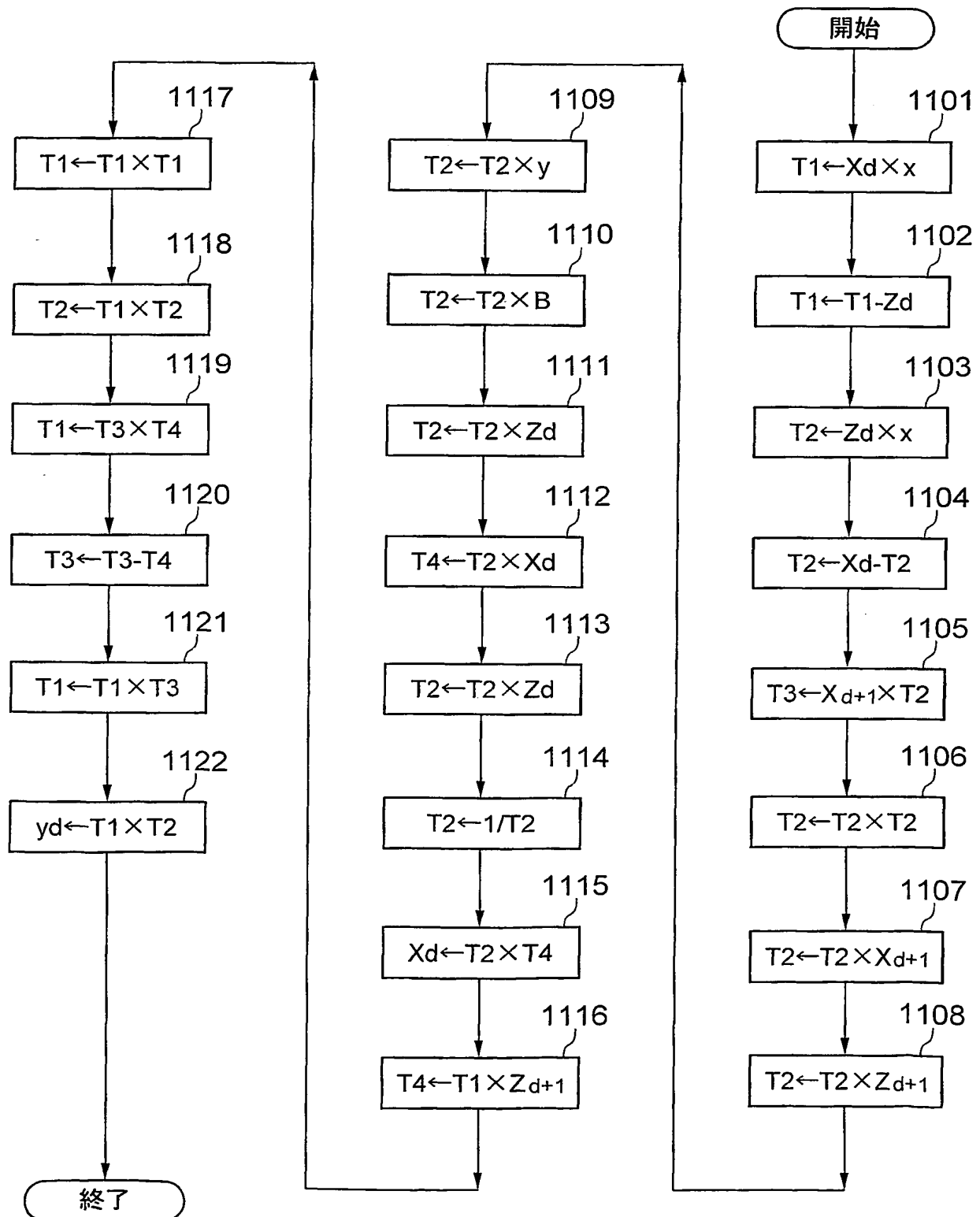
FIG. 10





11/45

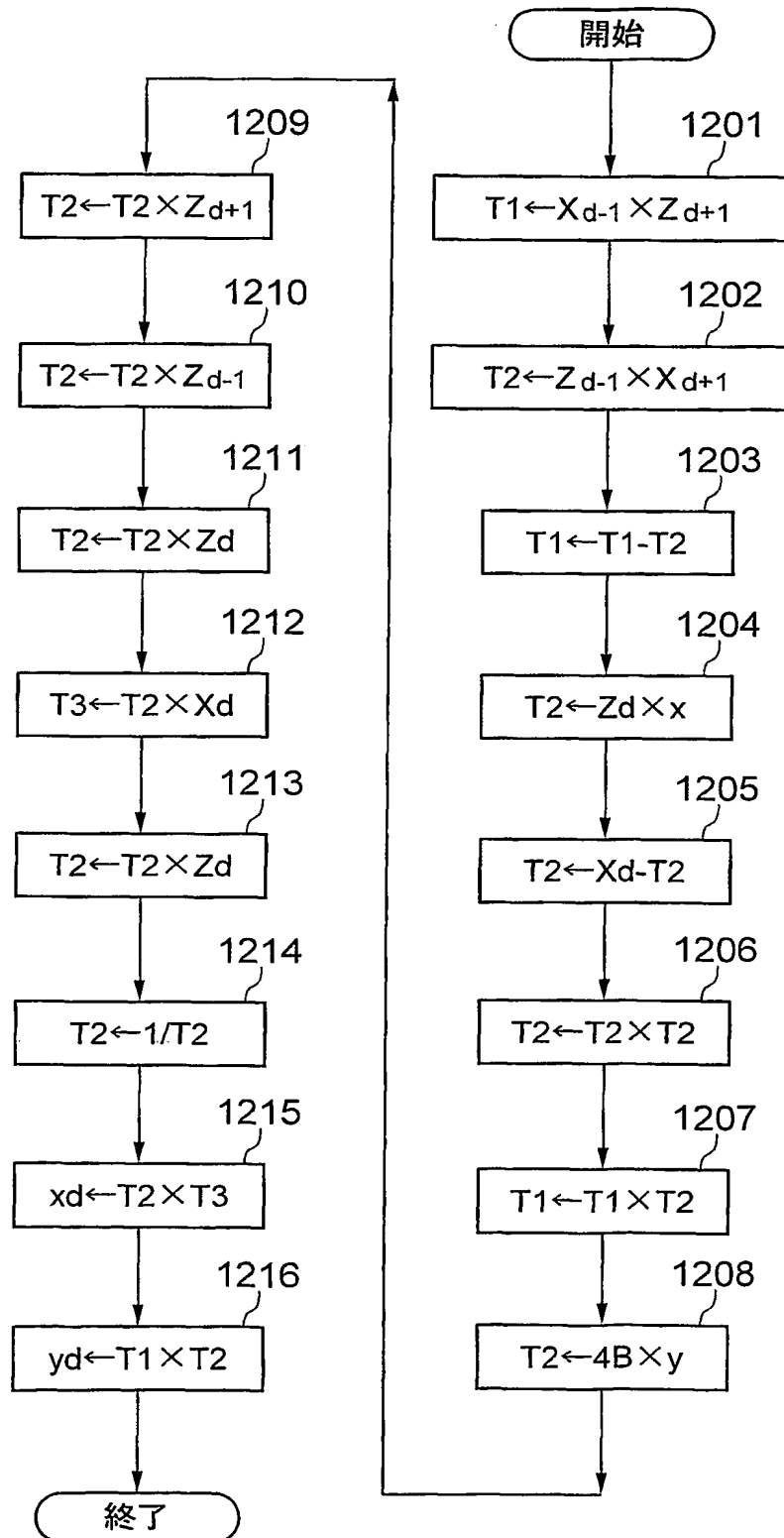
FIG. 11





12/45

FIG. 12





13/45

FIG. 13

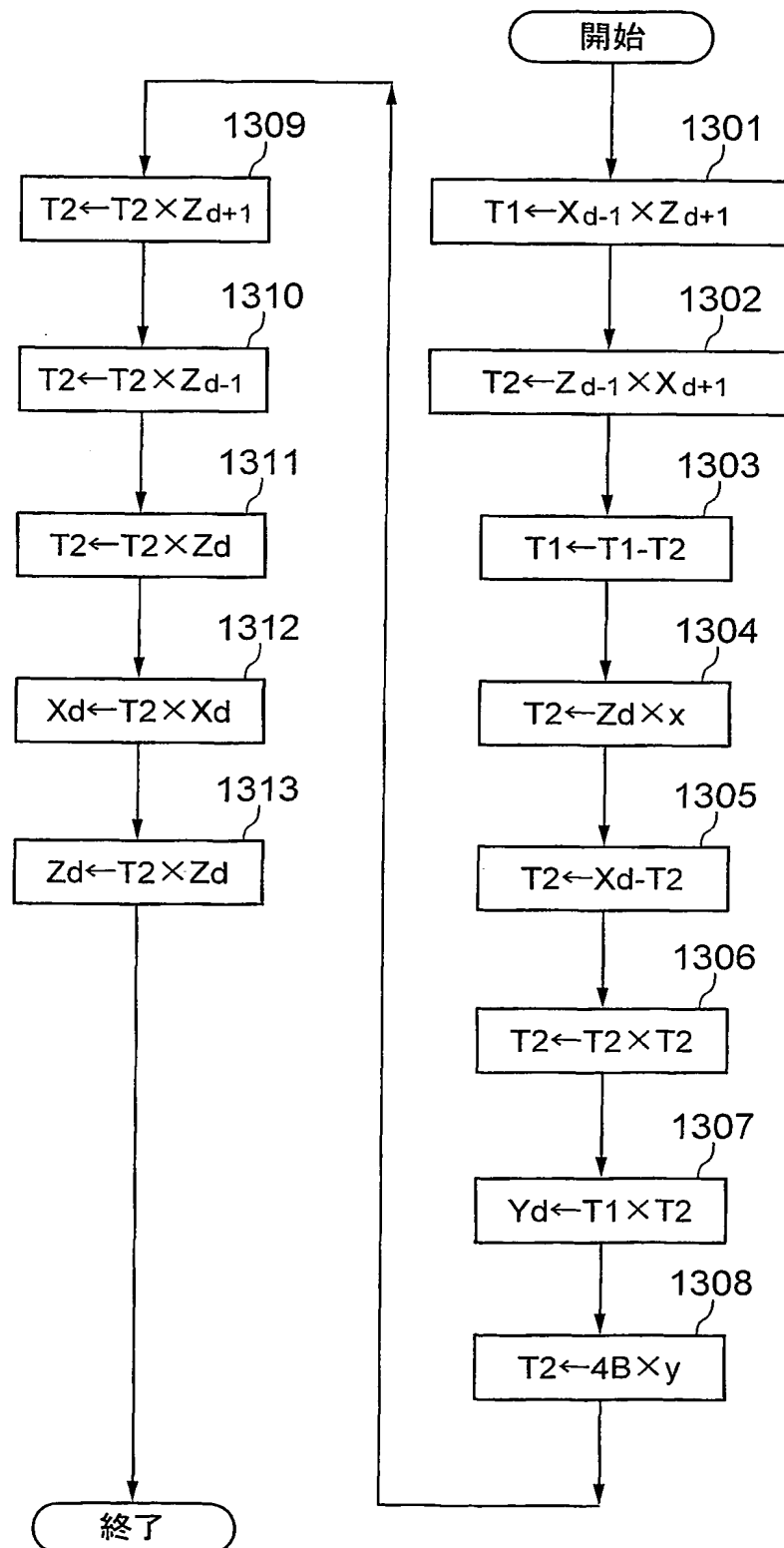
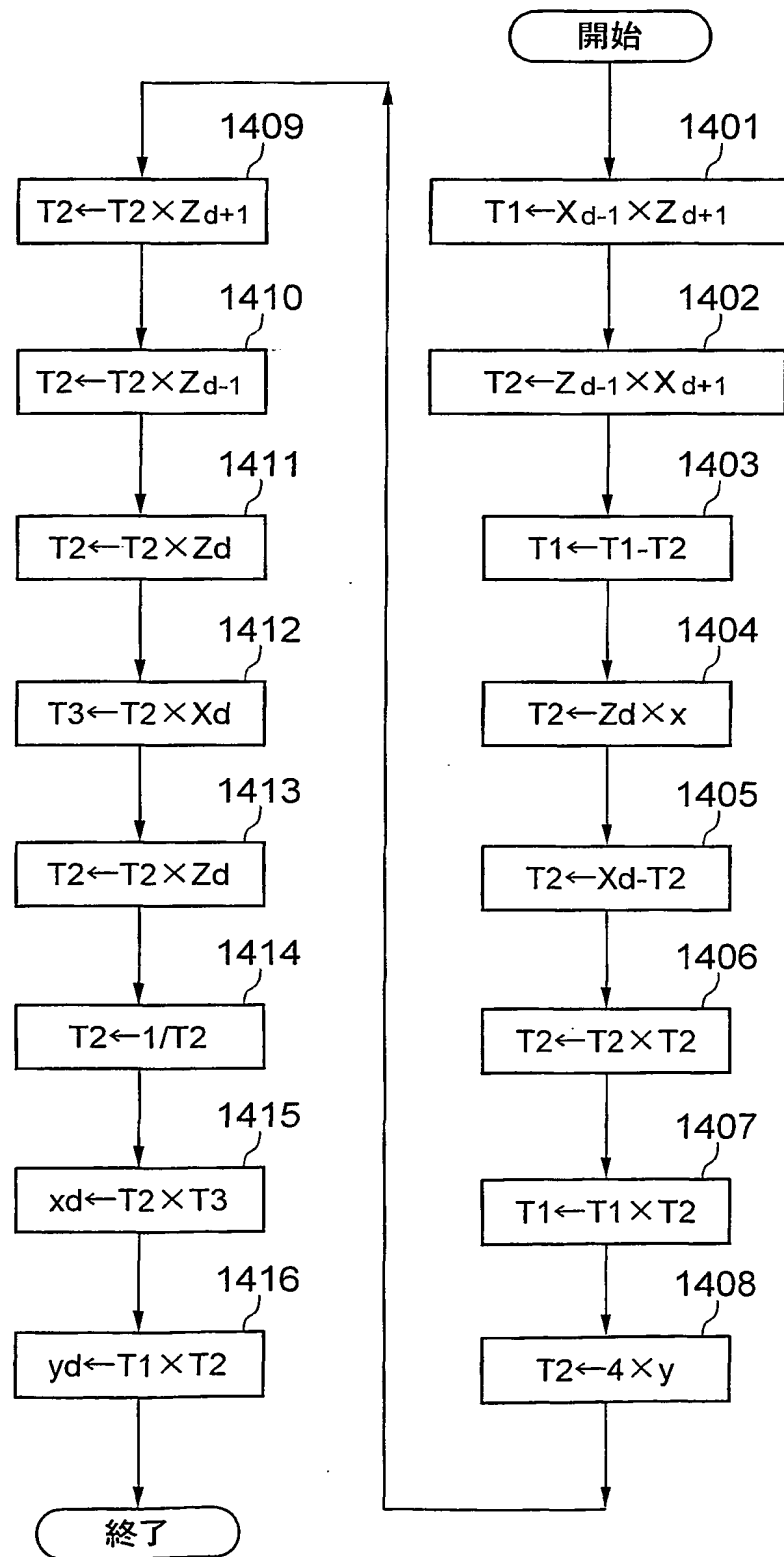




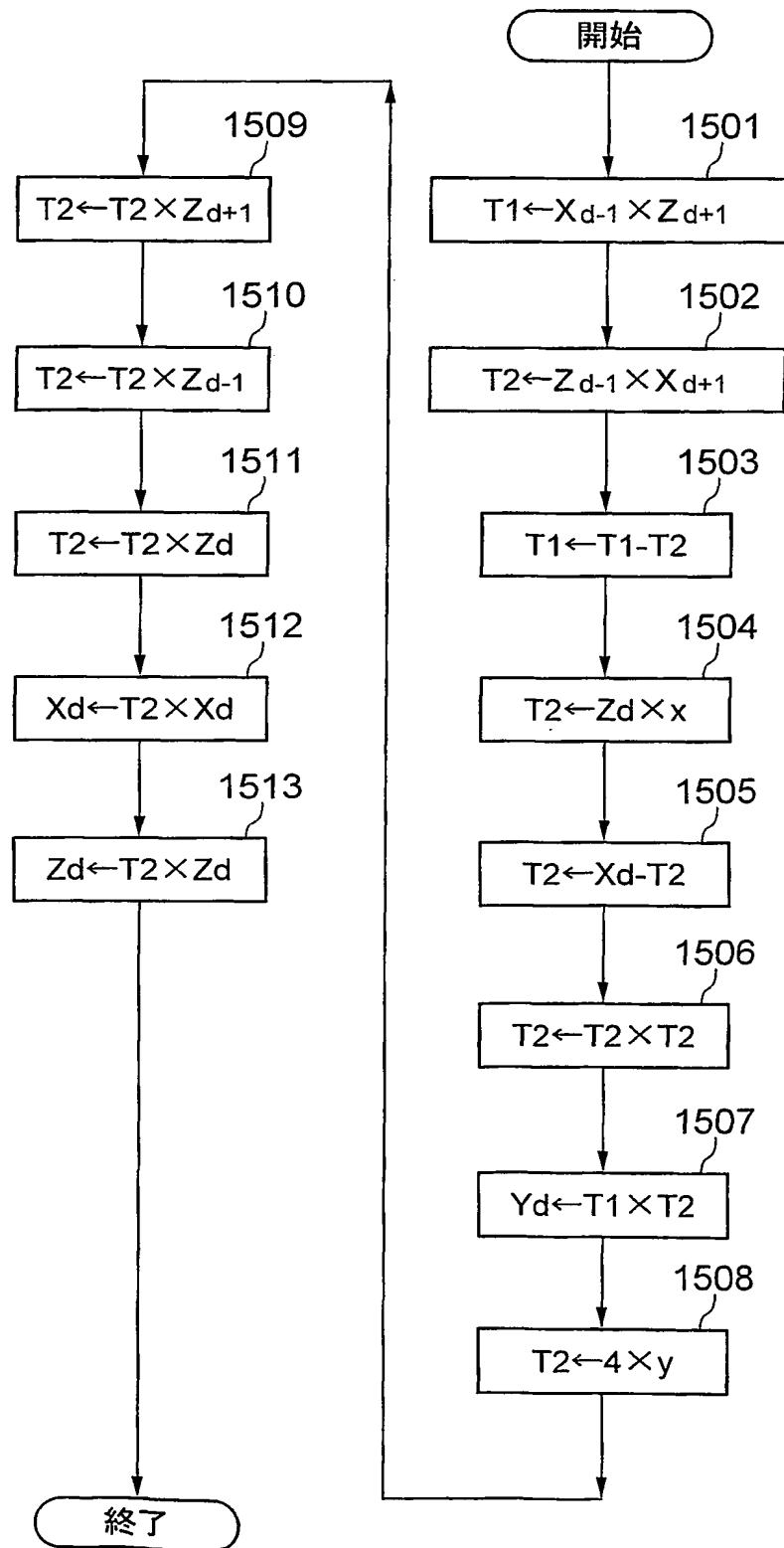
FIG. 14





15/45

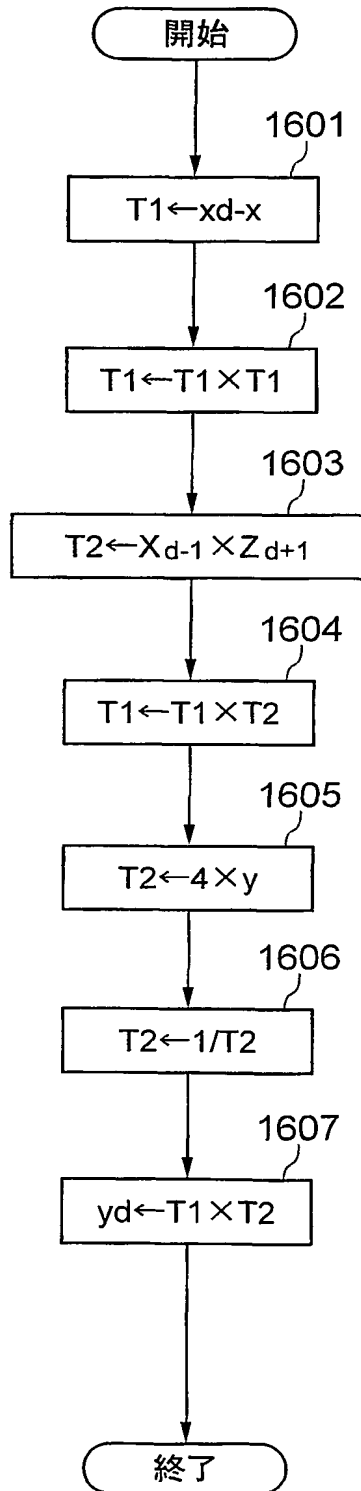
FIG. 15





16/45

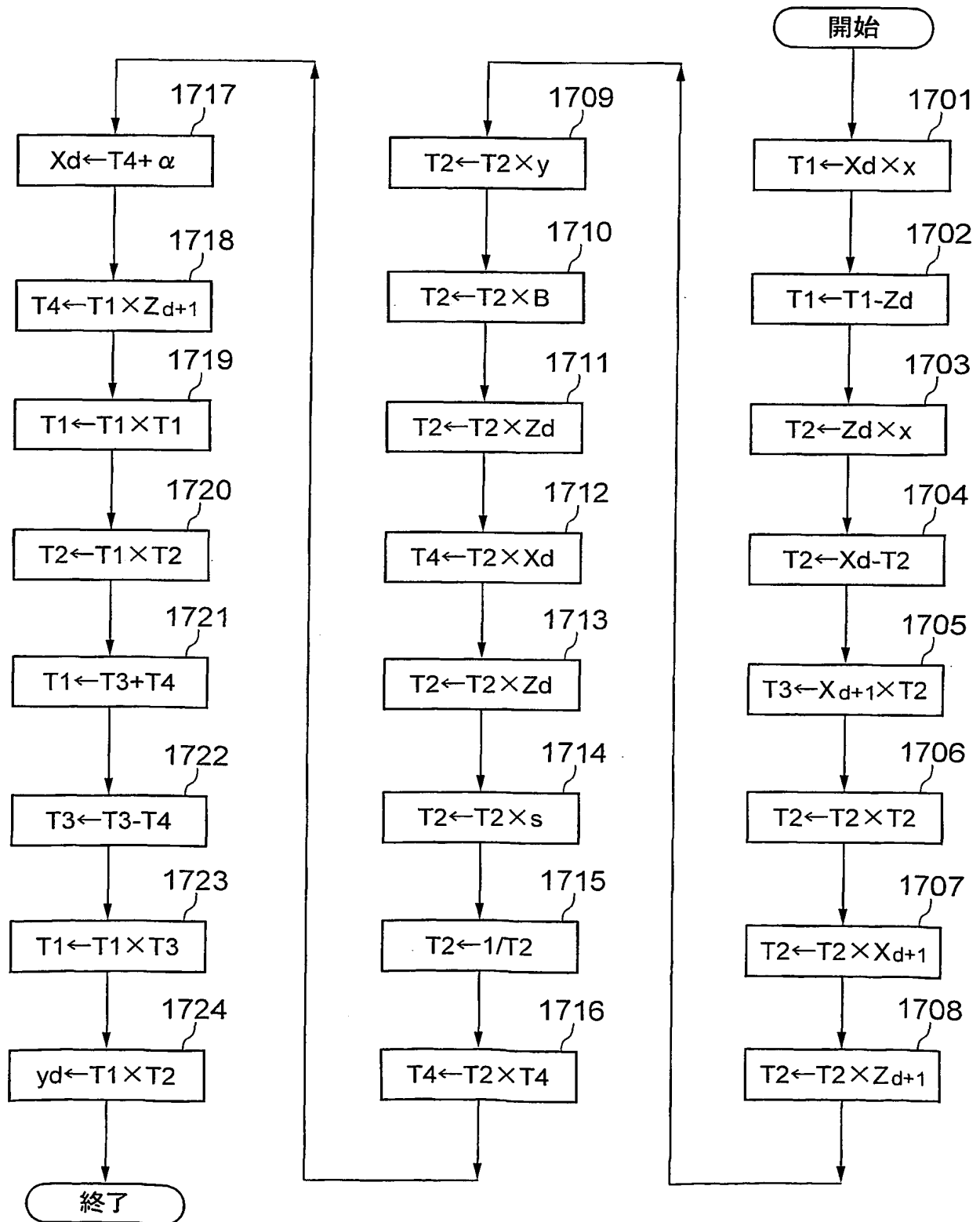
FIG. 16





17/45

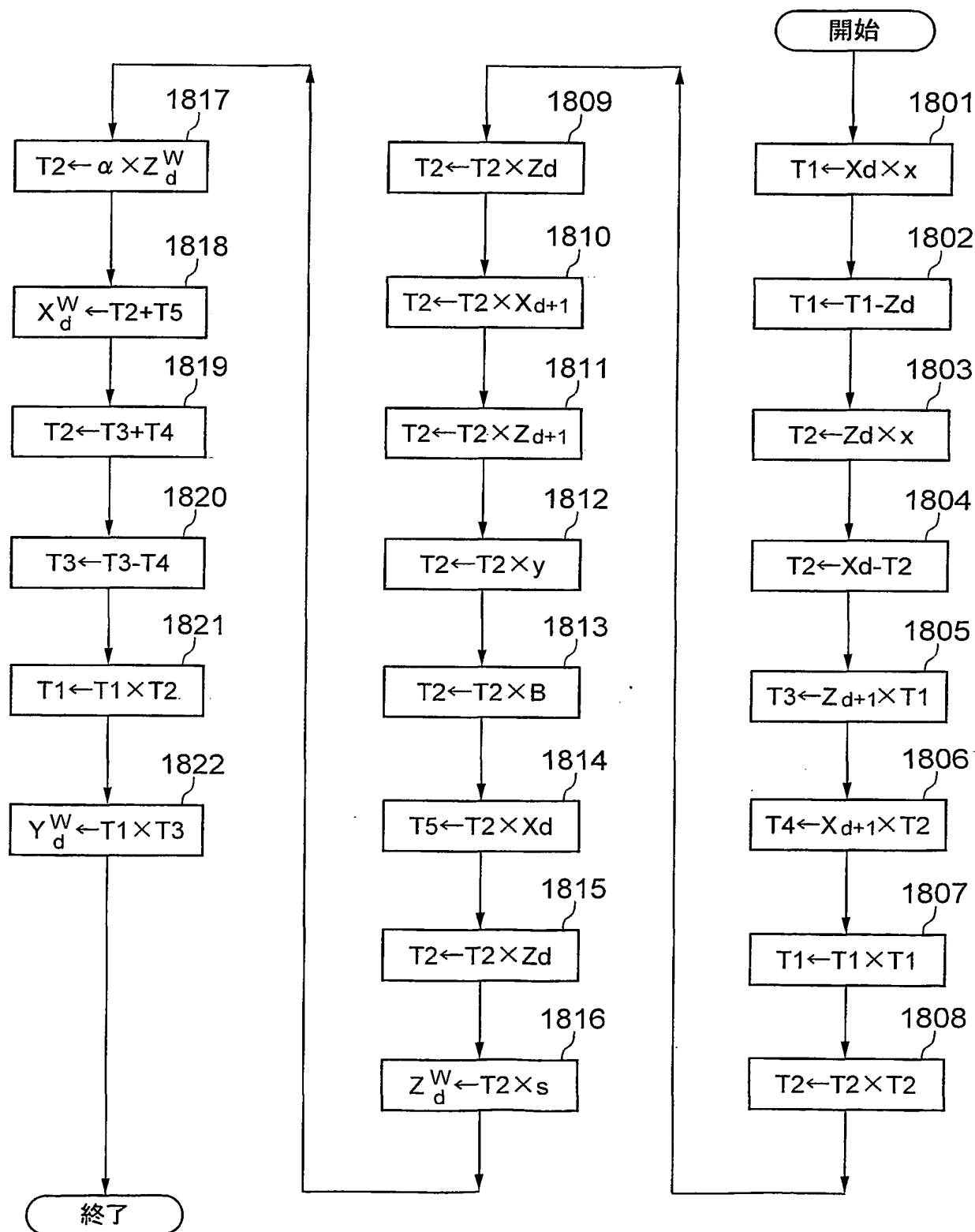
FIG. 17





18/45

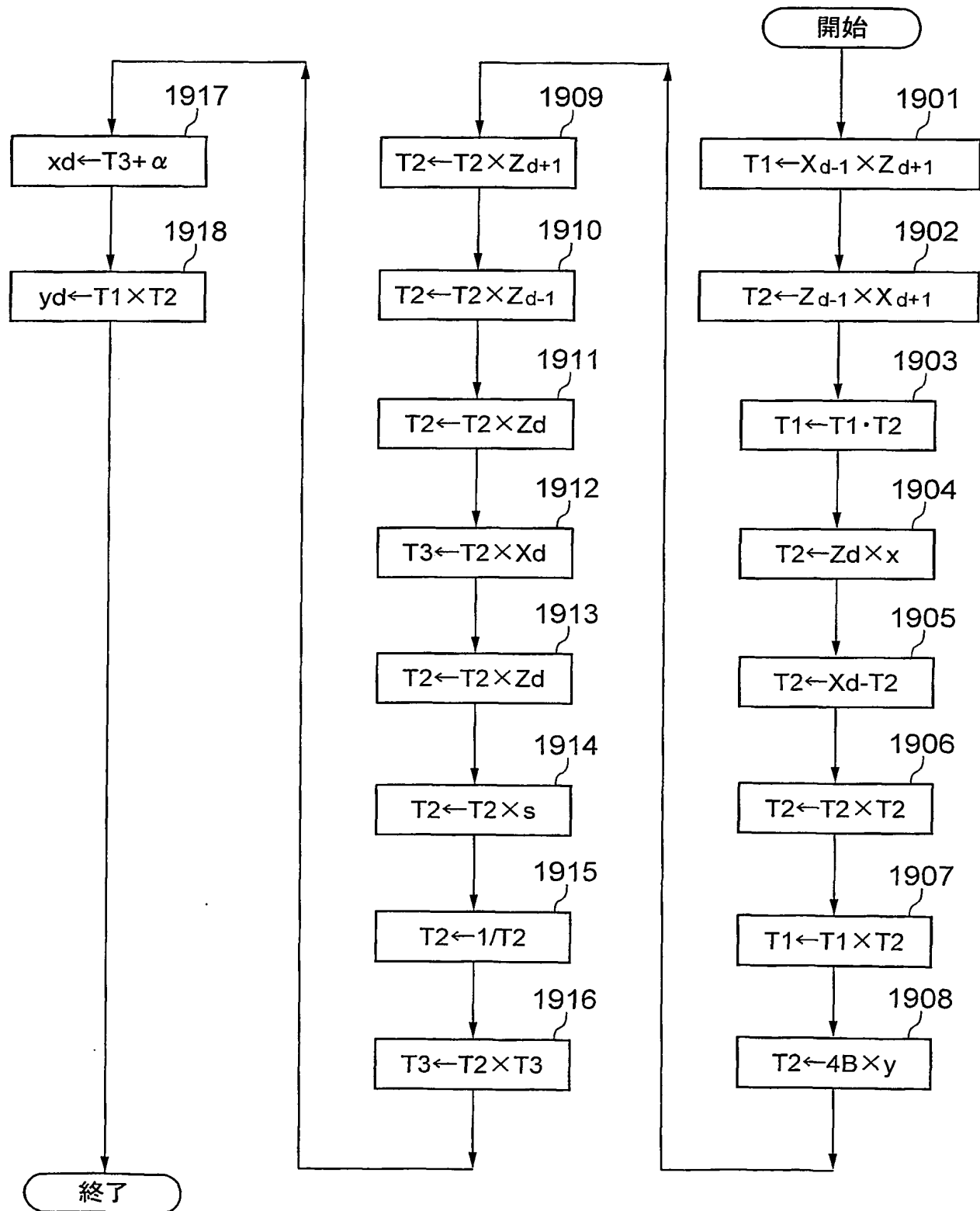
FIG. 18





19/45

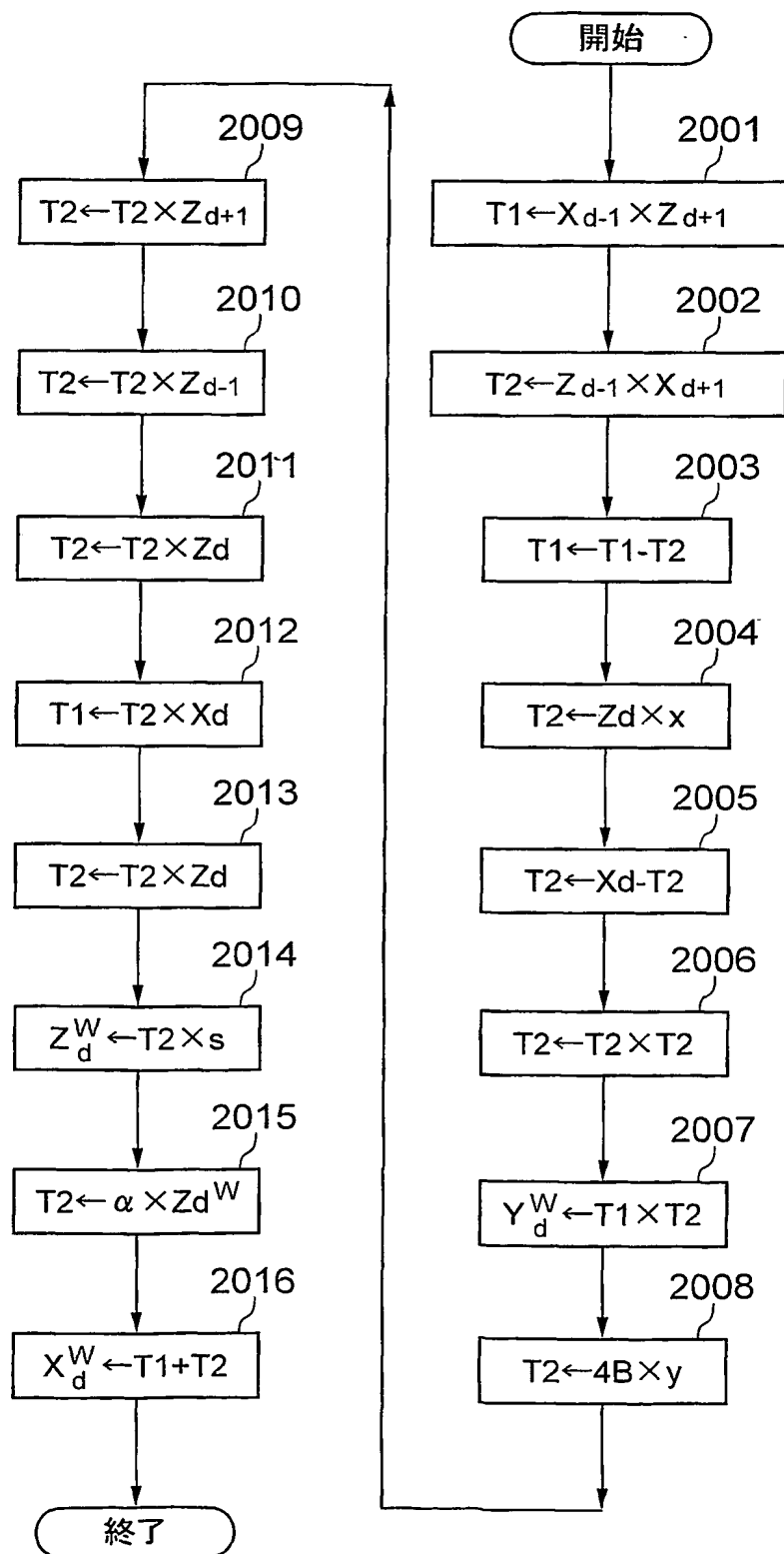
FIG. 19





20/45

FIG. 20





21/45

FIG. 21

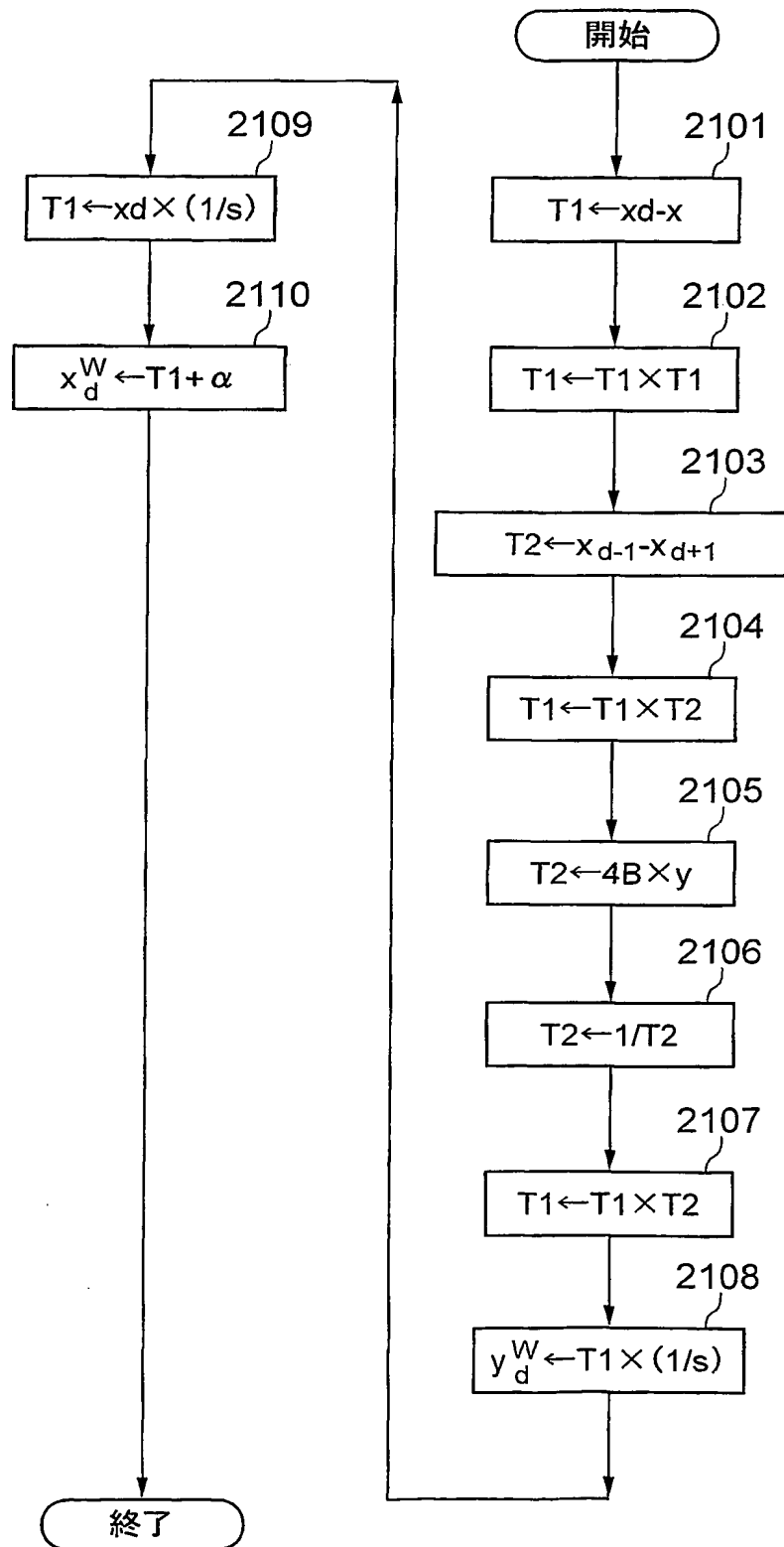




FIG. 22

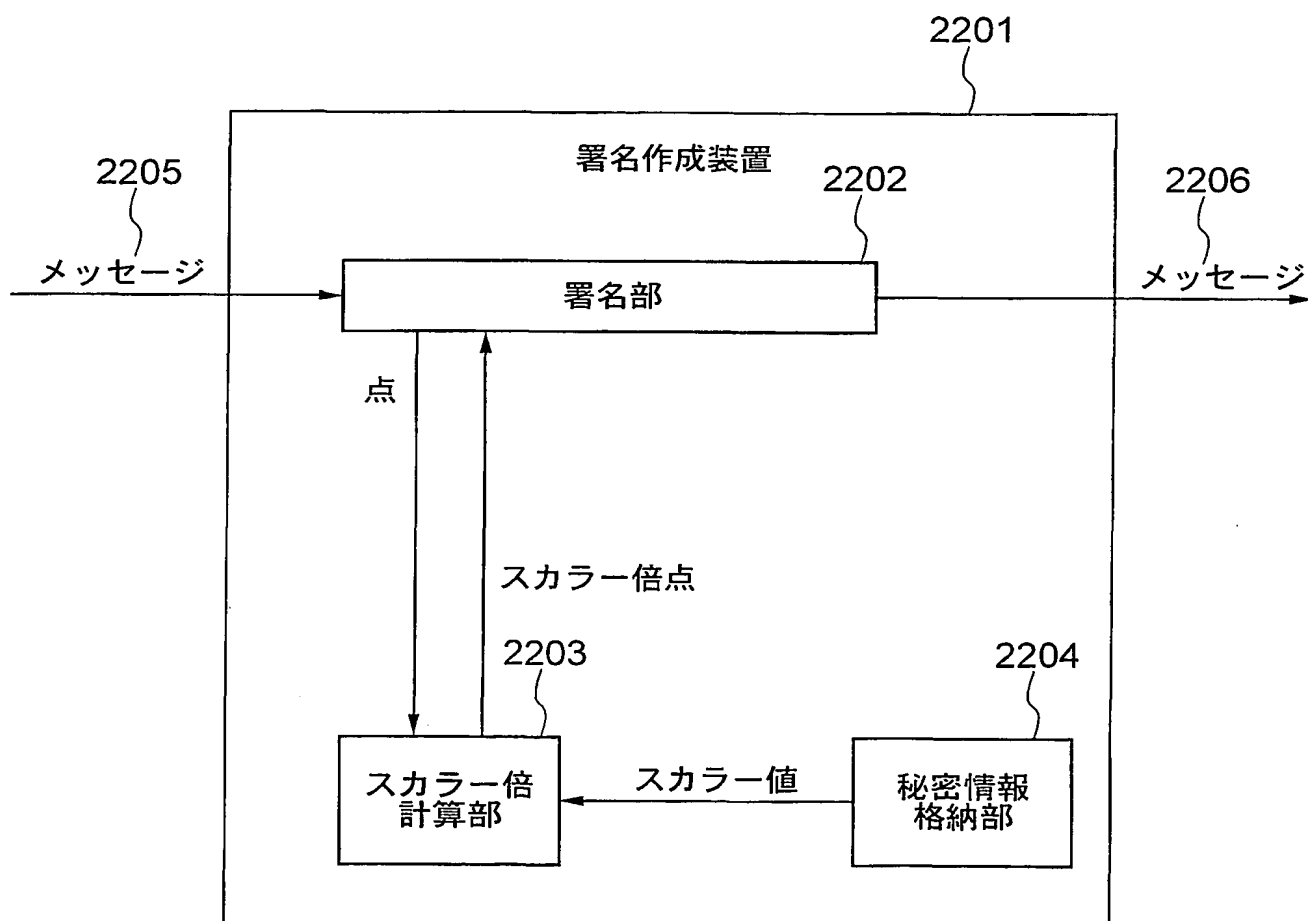
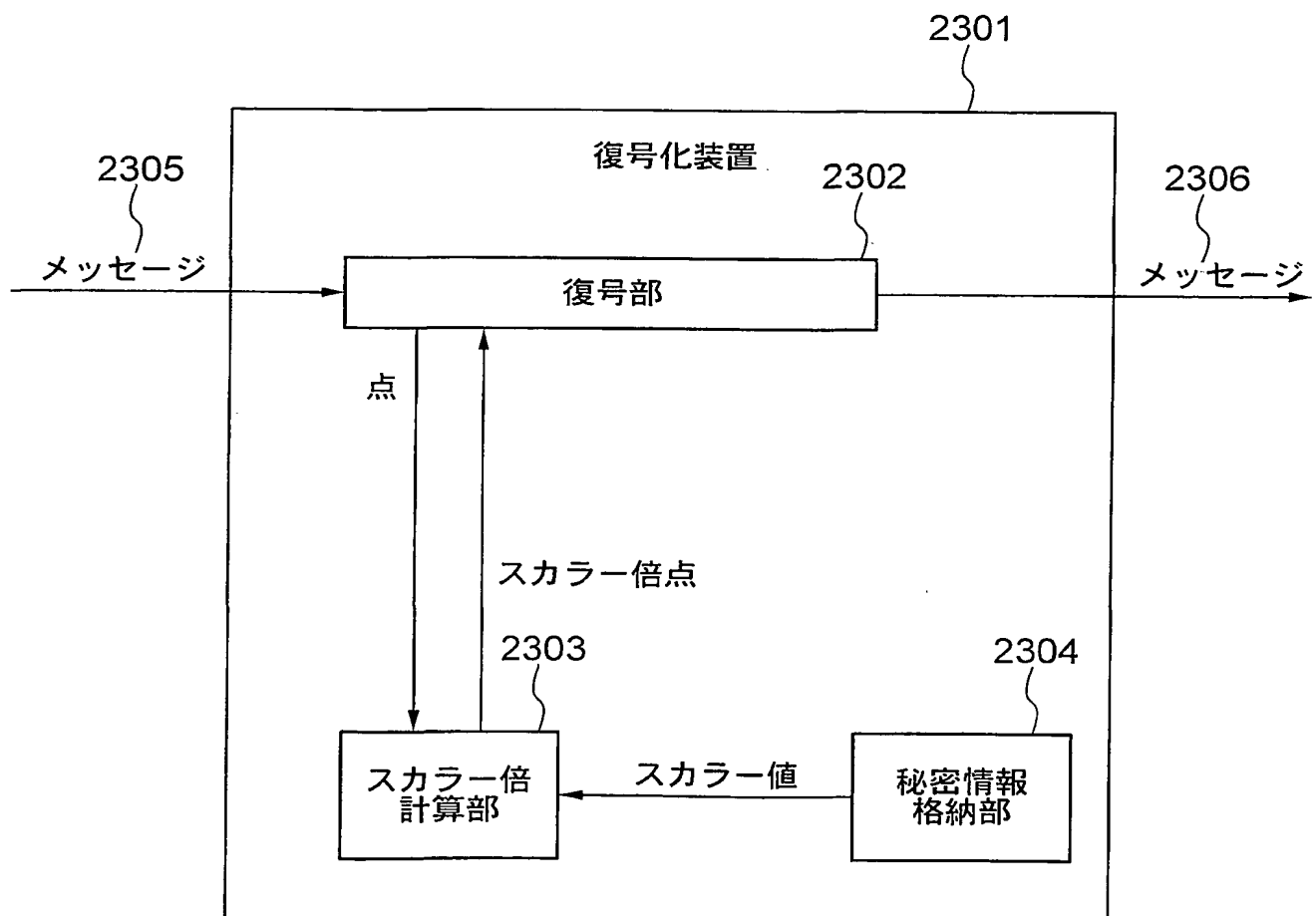




FIG. 23





24/45

FIG. 24

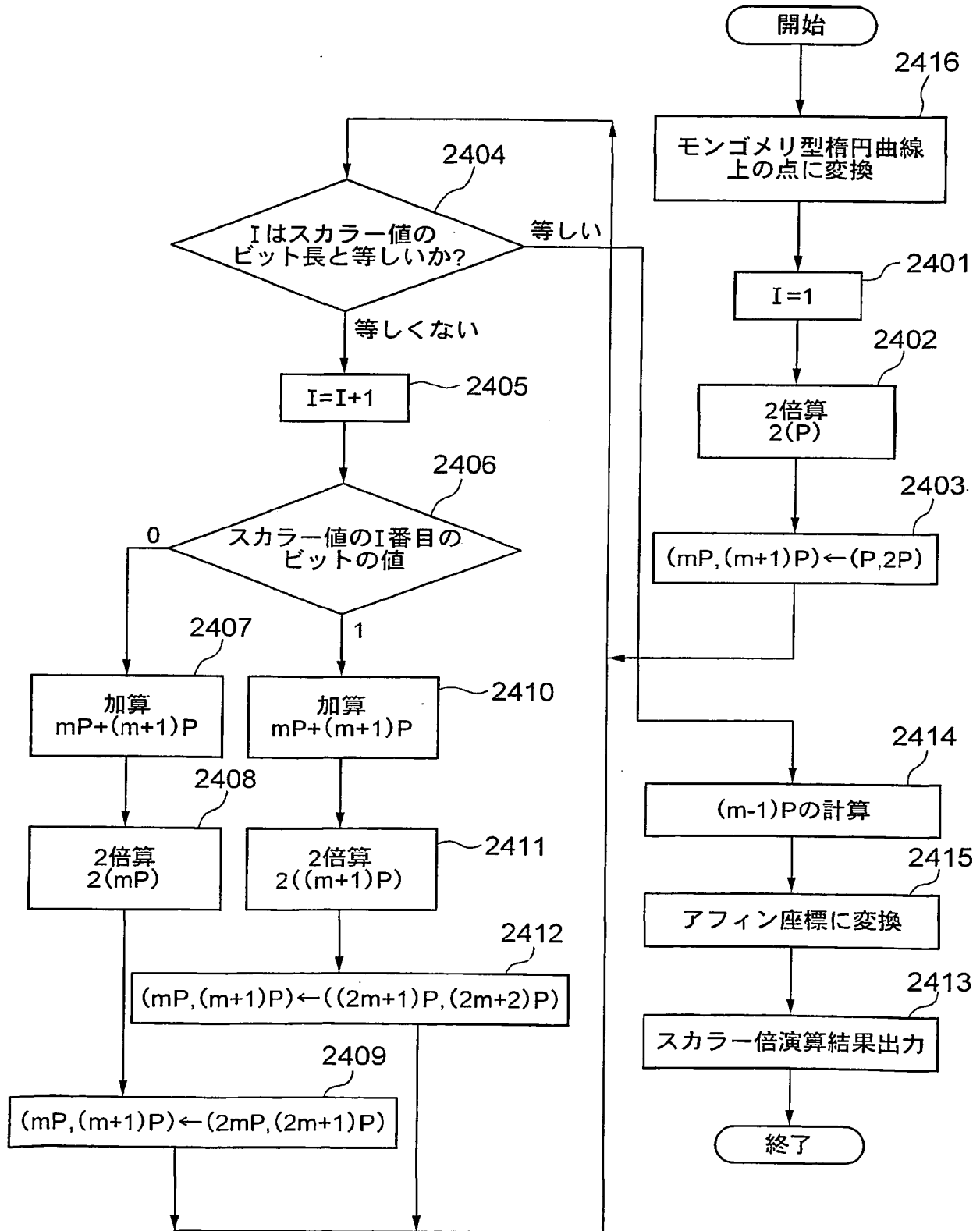
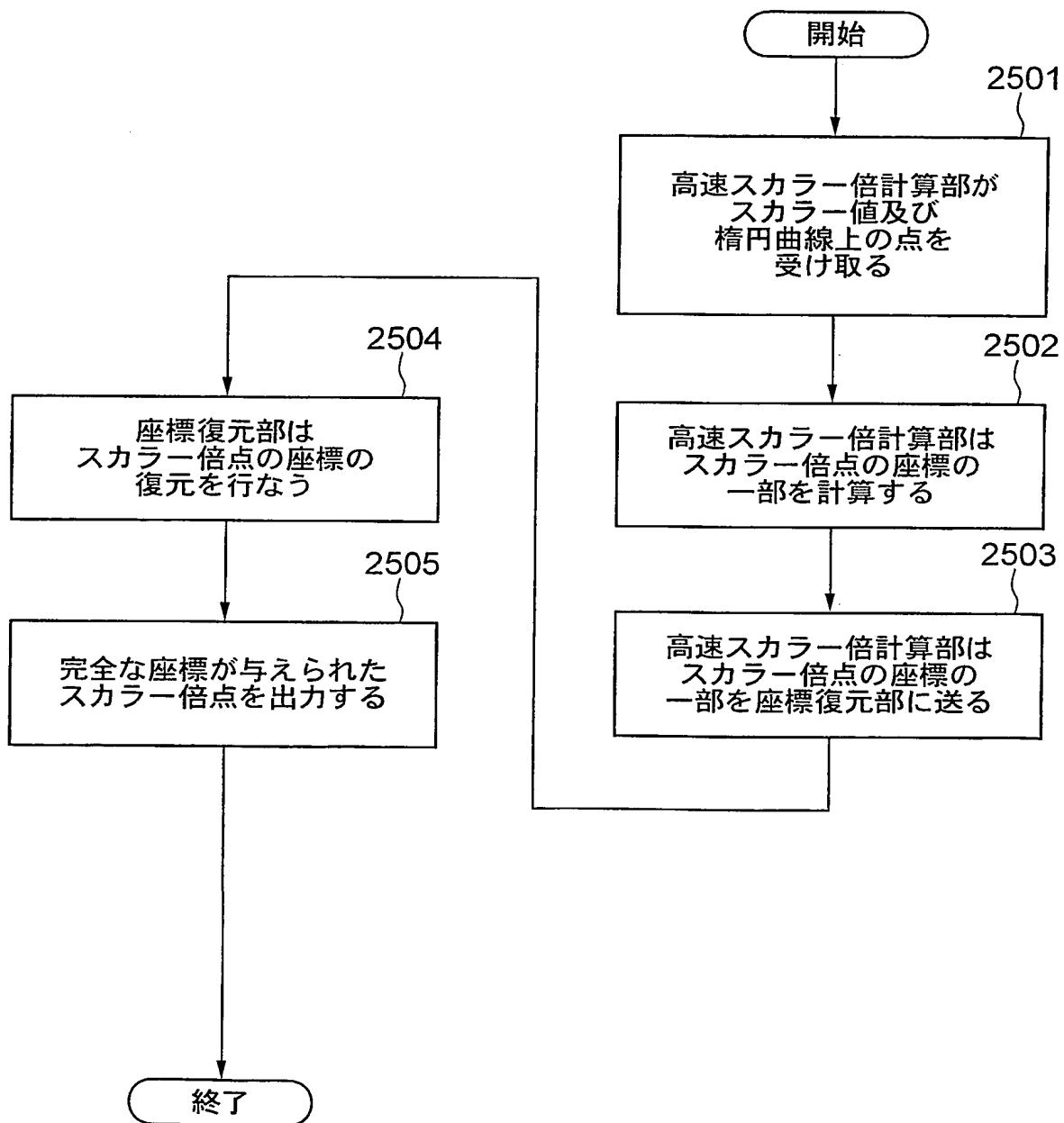




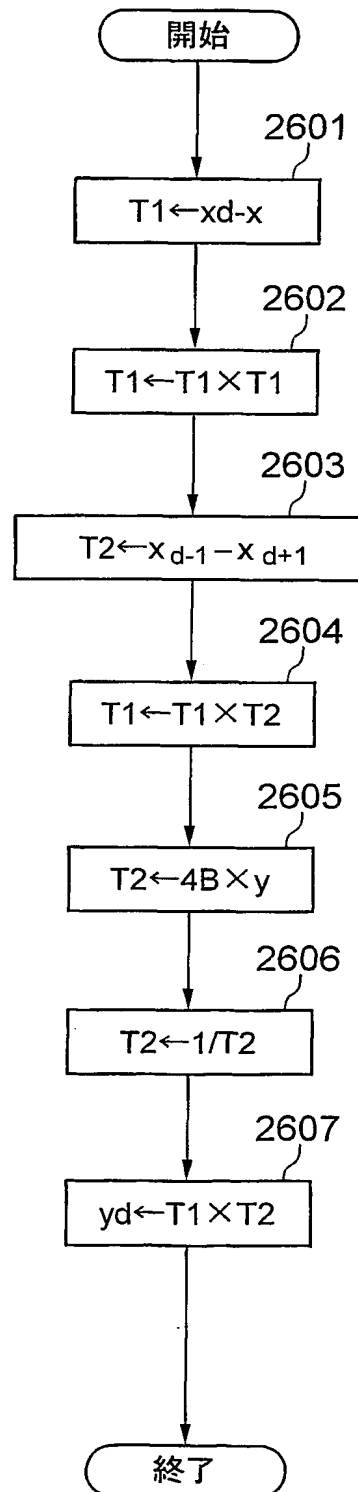
FIG. 25





26/45

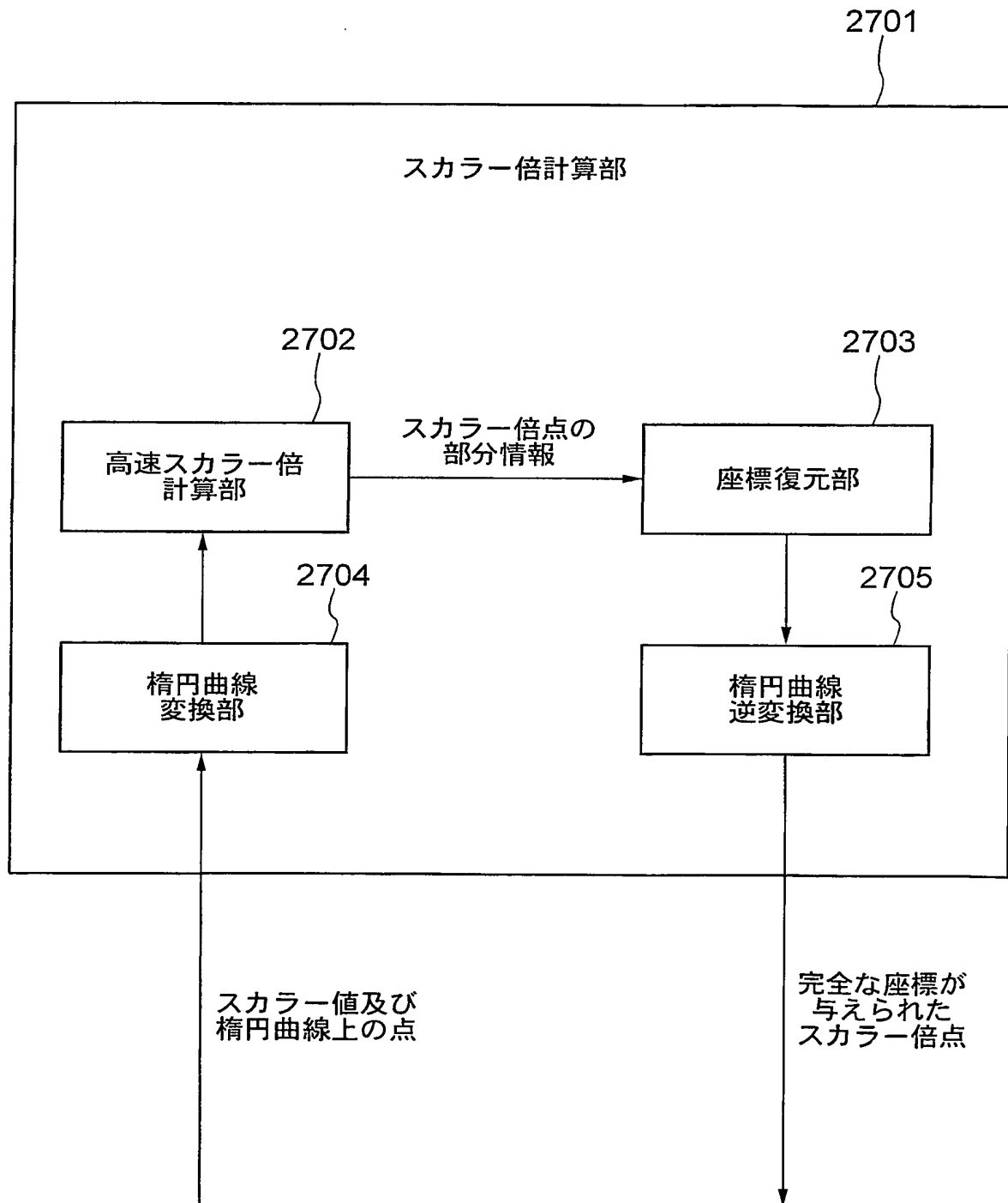
FIG. 26





27/45

FIG. 27





28/45

FIG. 28

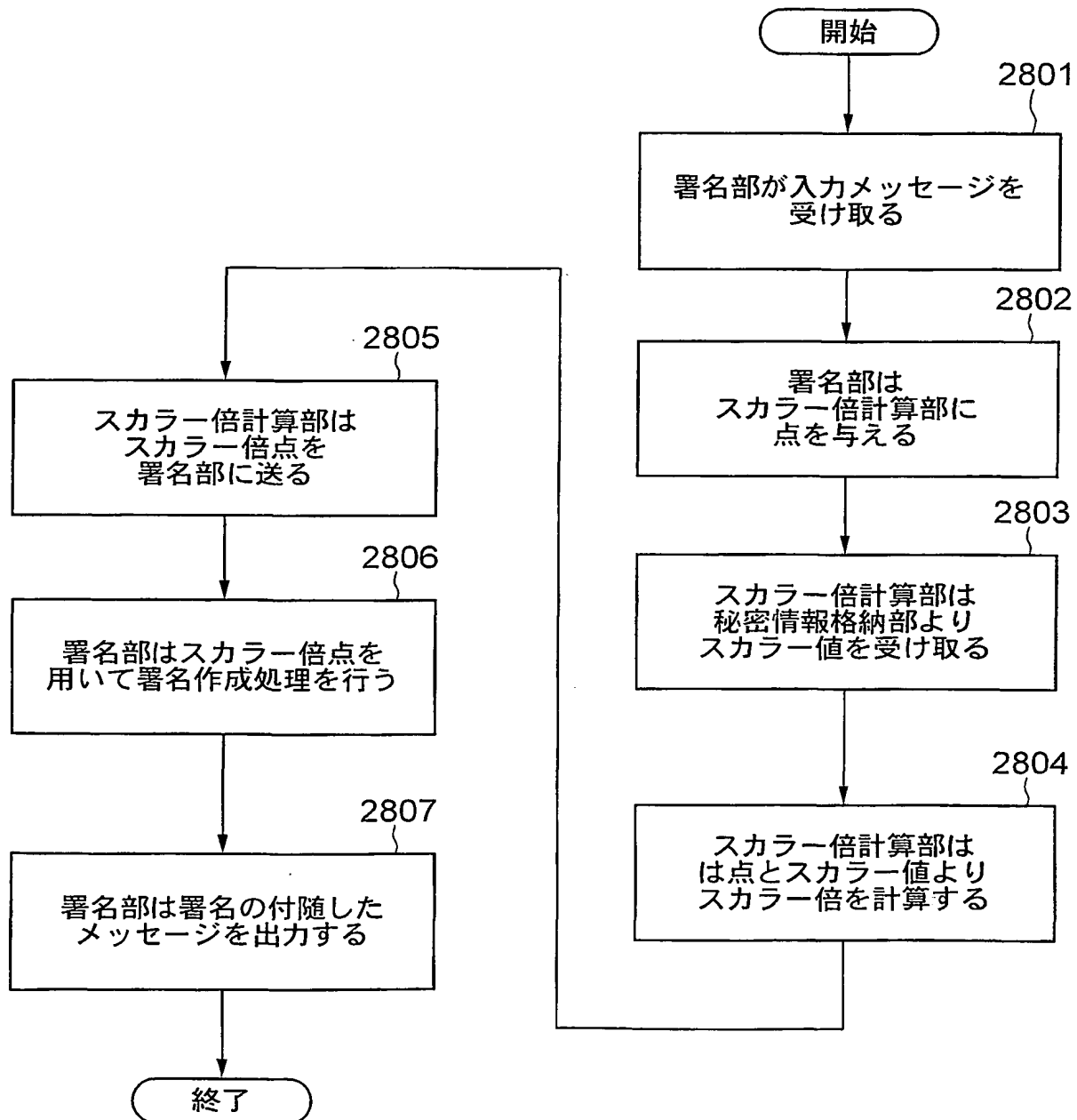




FIG. 29

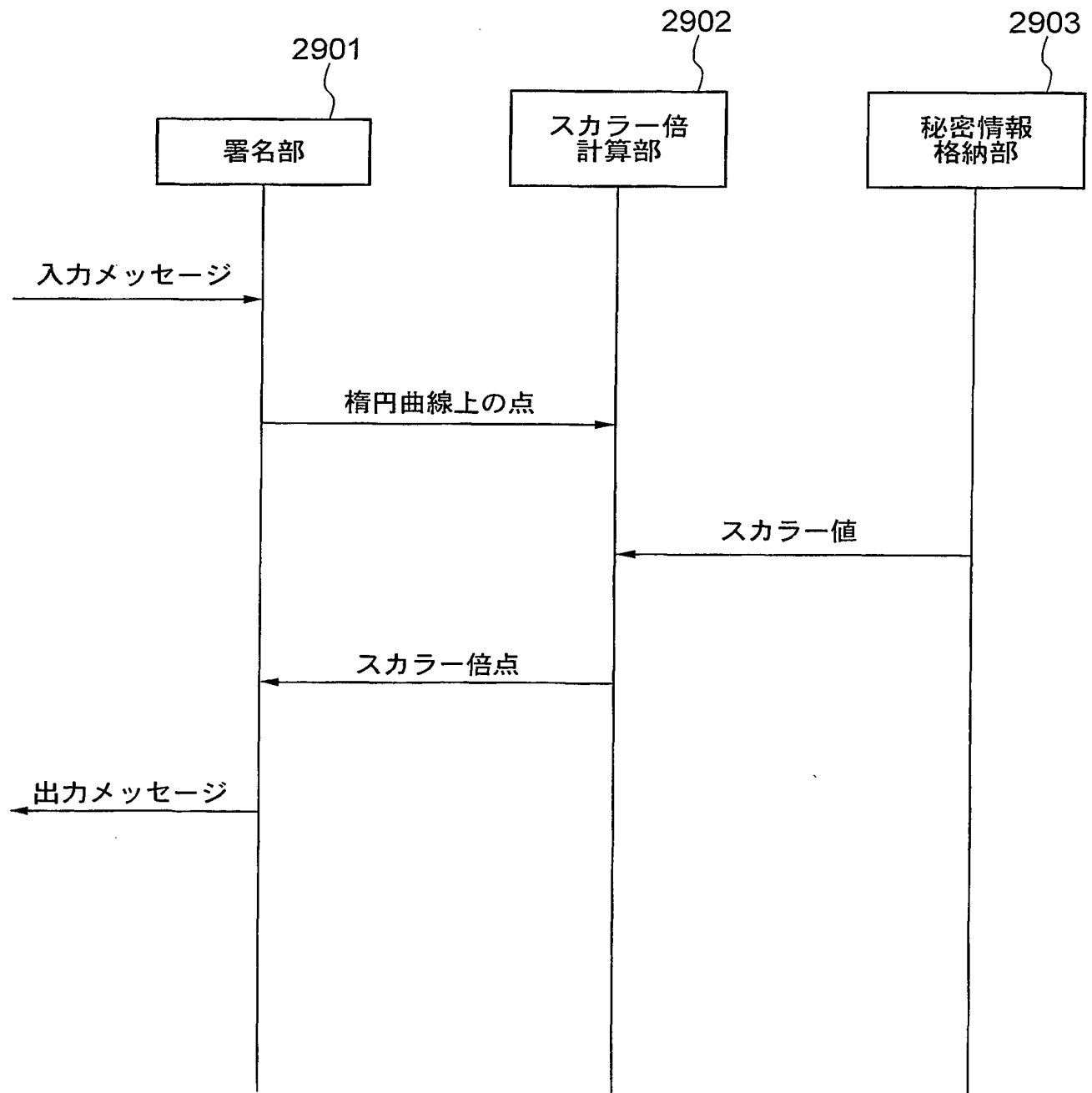




FIG. 30

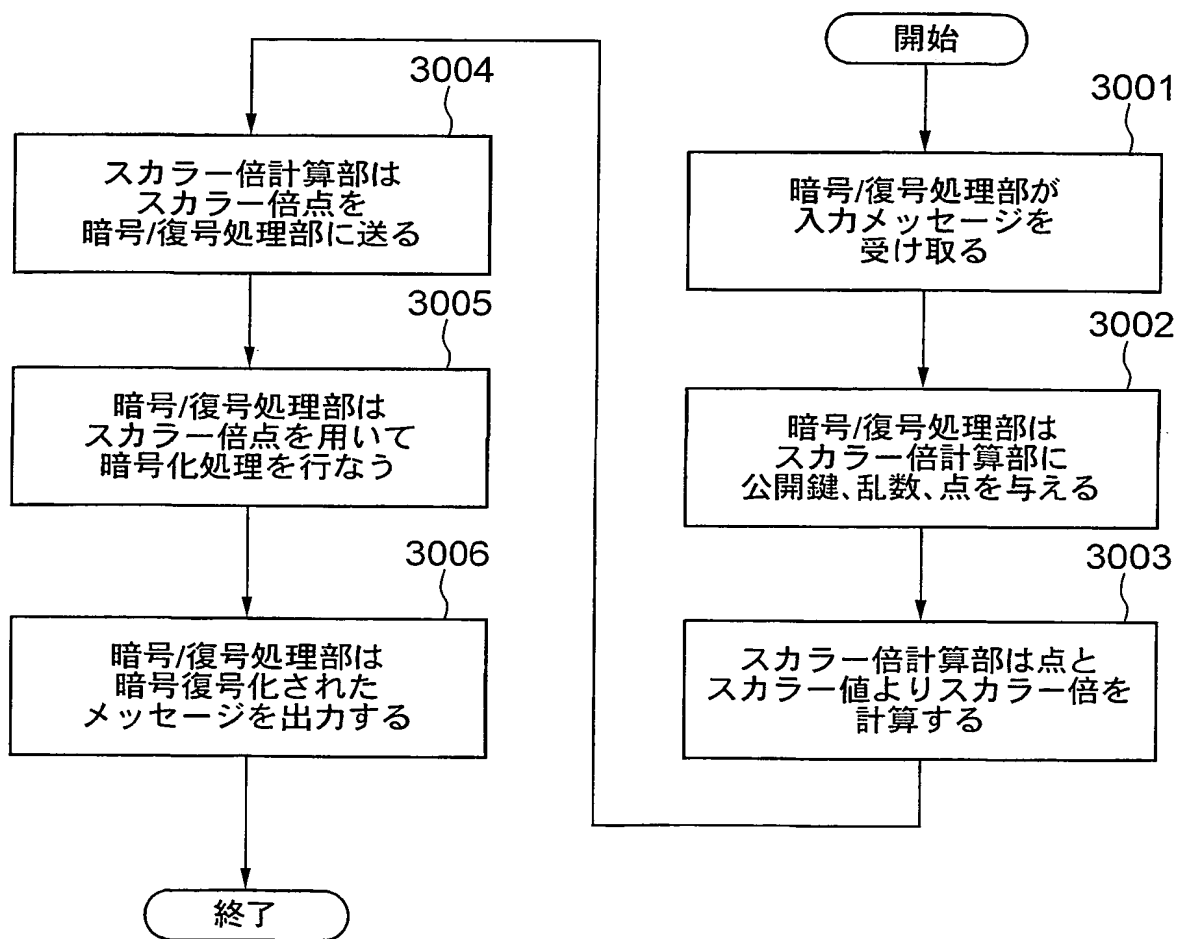
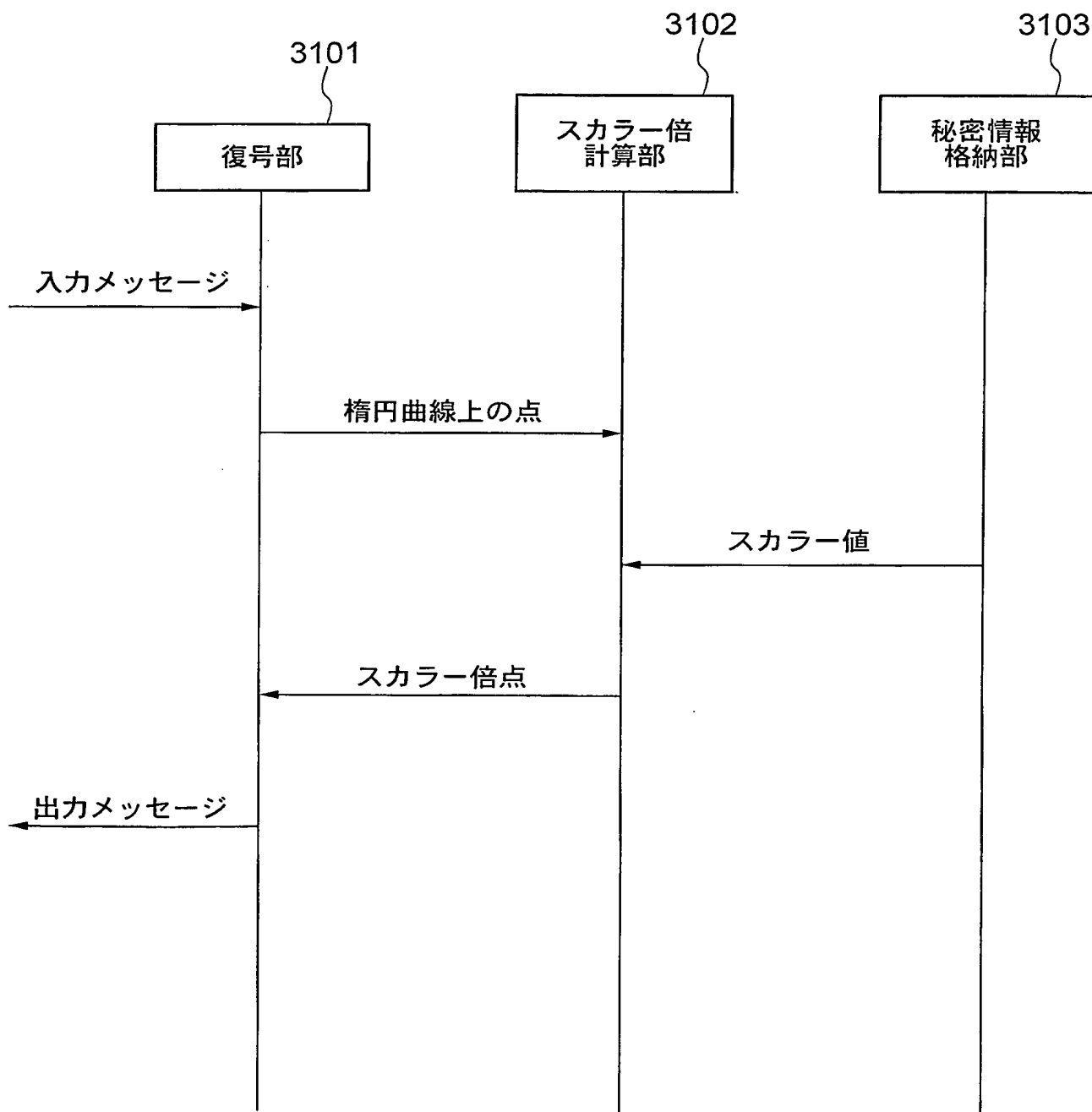




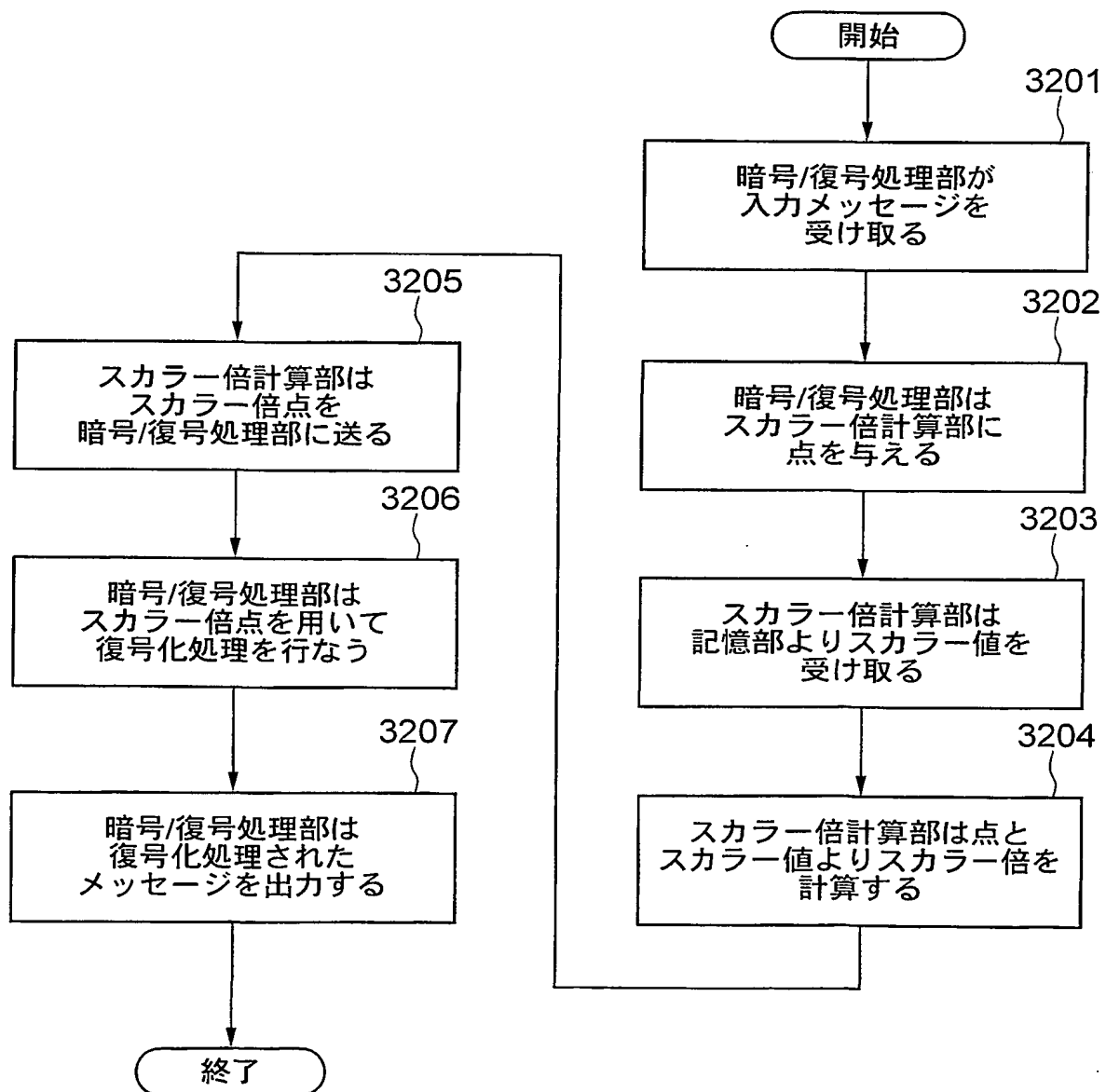
FIG. 31





32/45

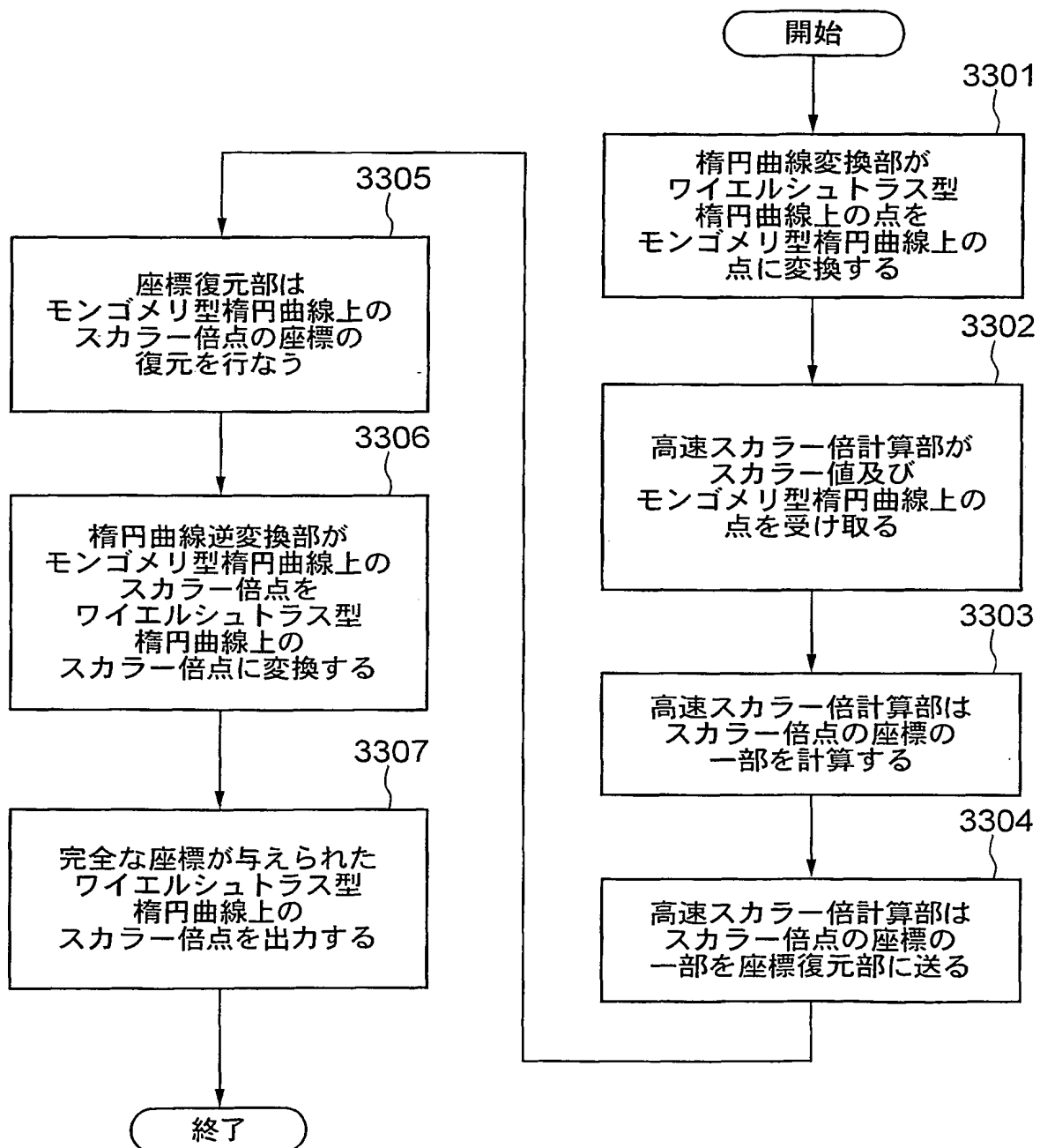
FIG. 32





33/45

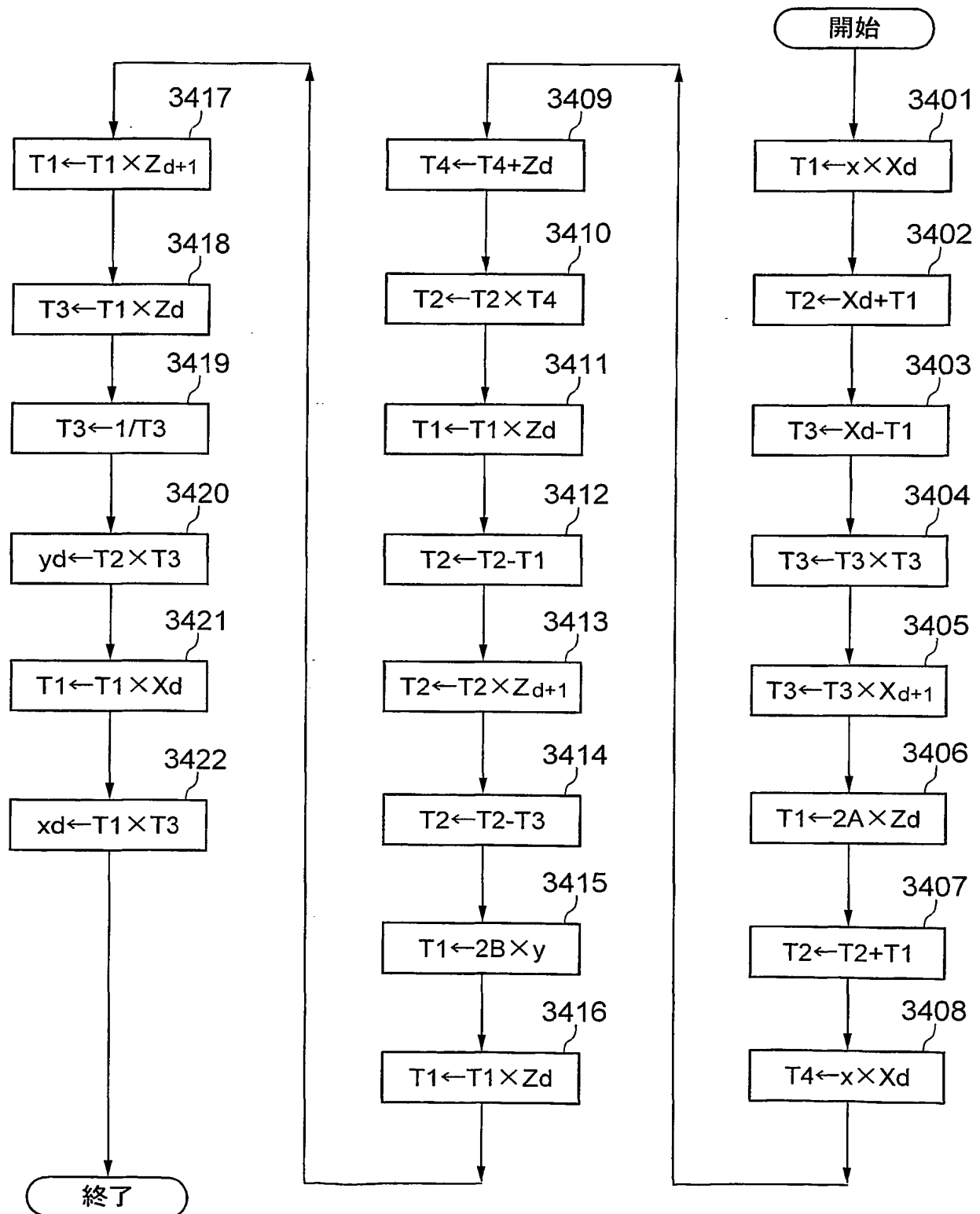
FIG. 33





34/45

FIG. 34





.

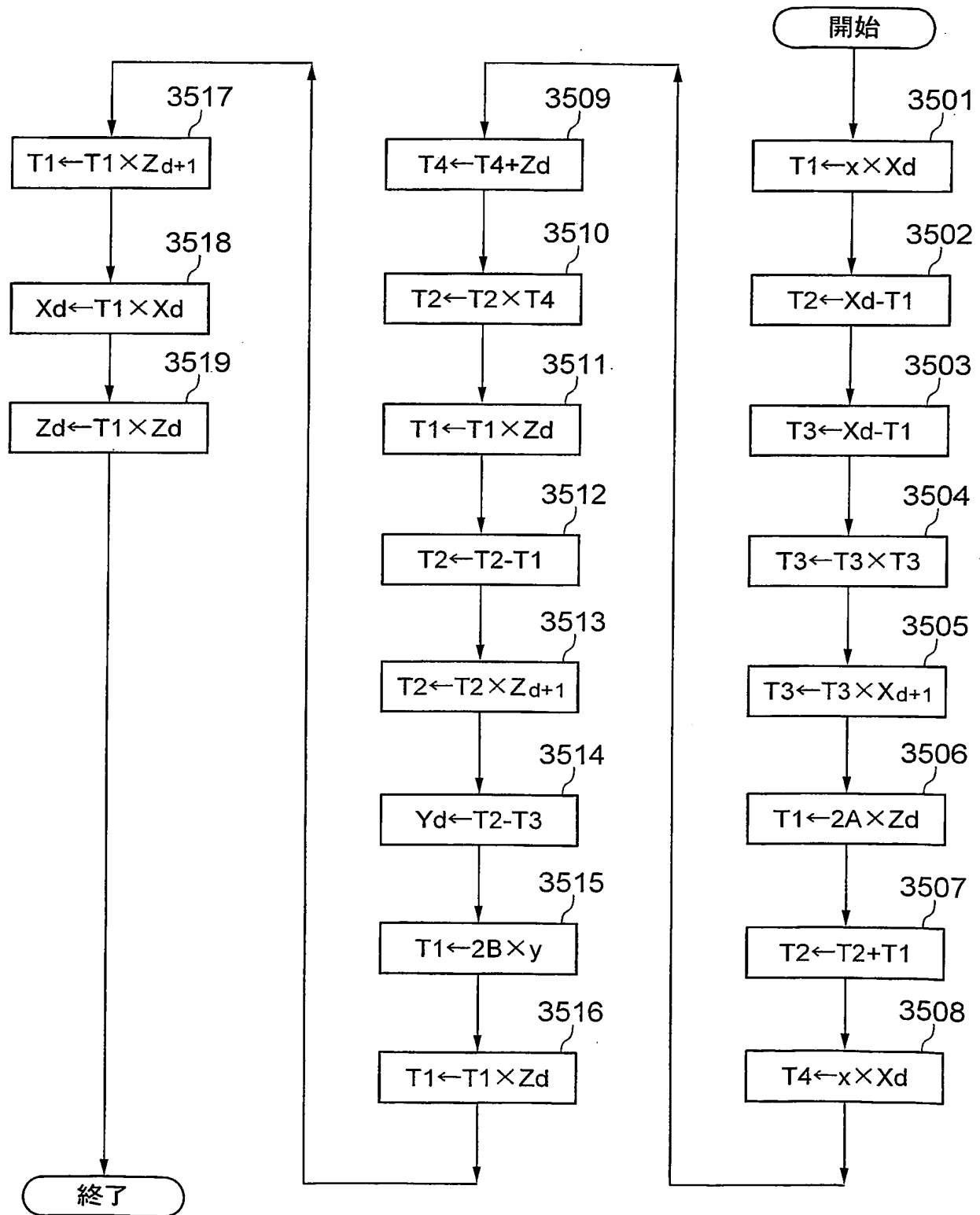
.

.

.

35/45

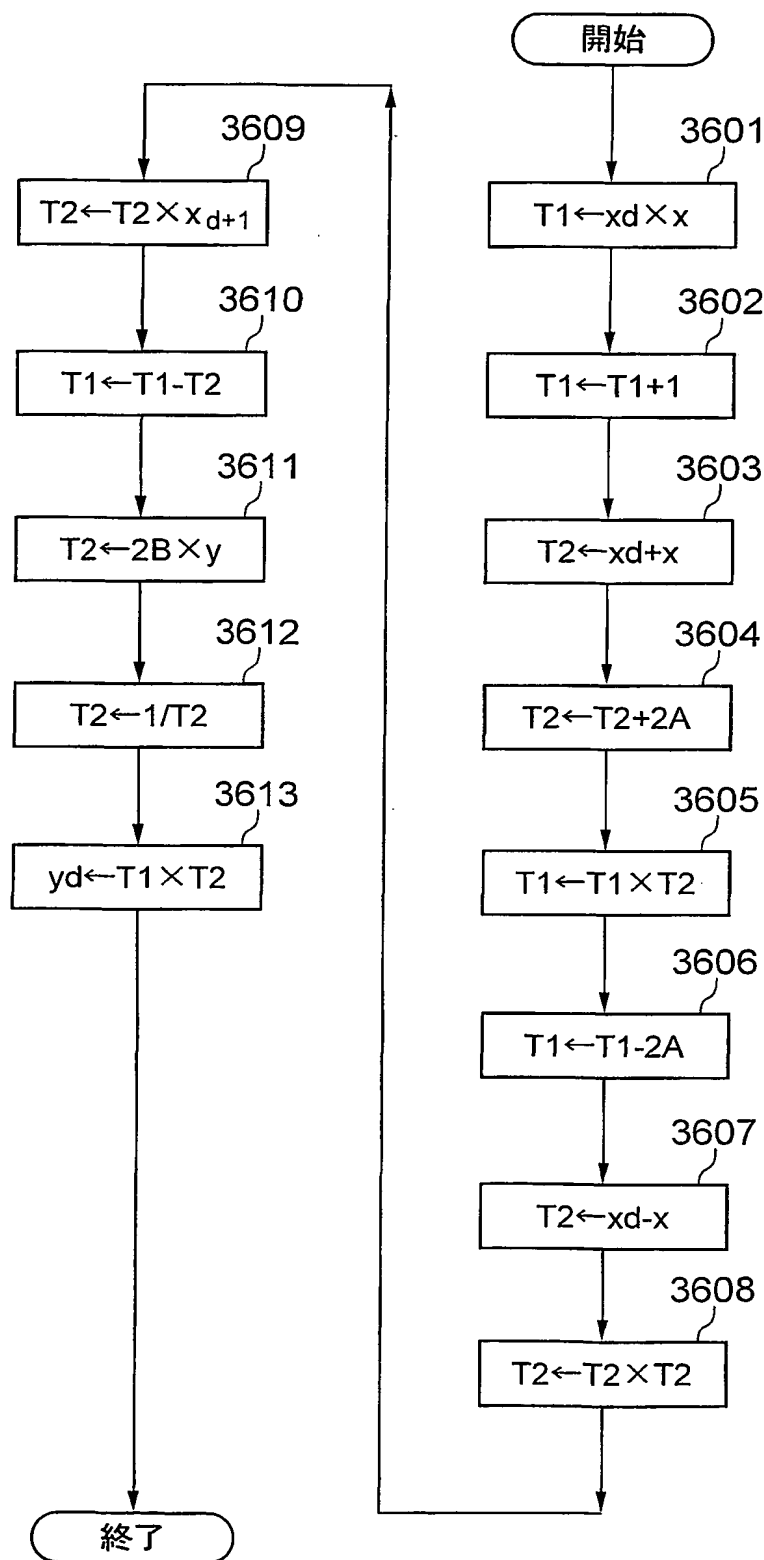
FIG. 35





36/45

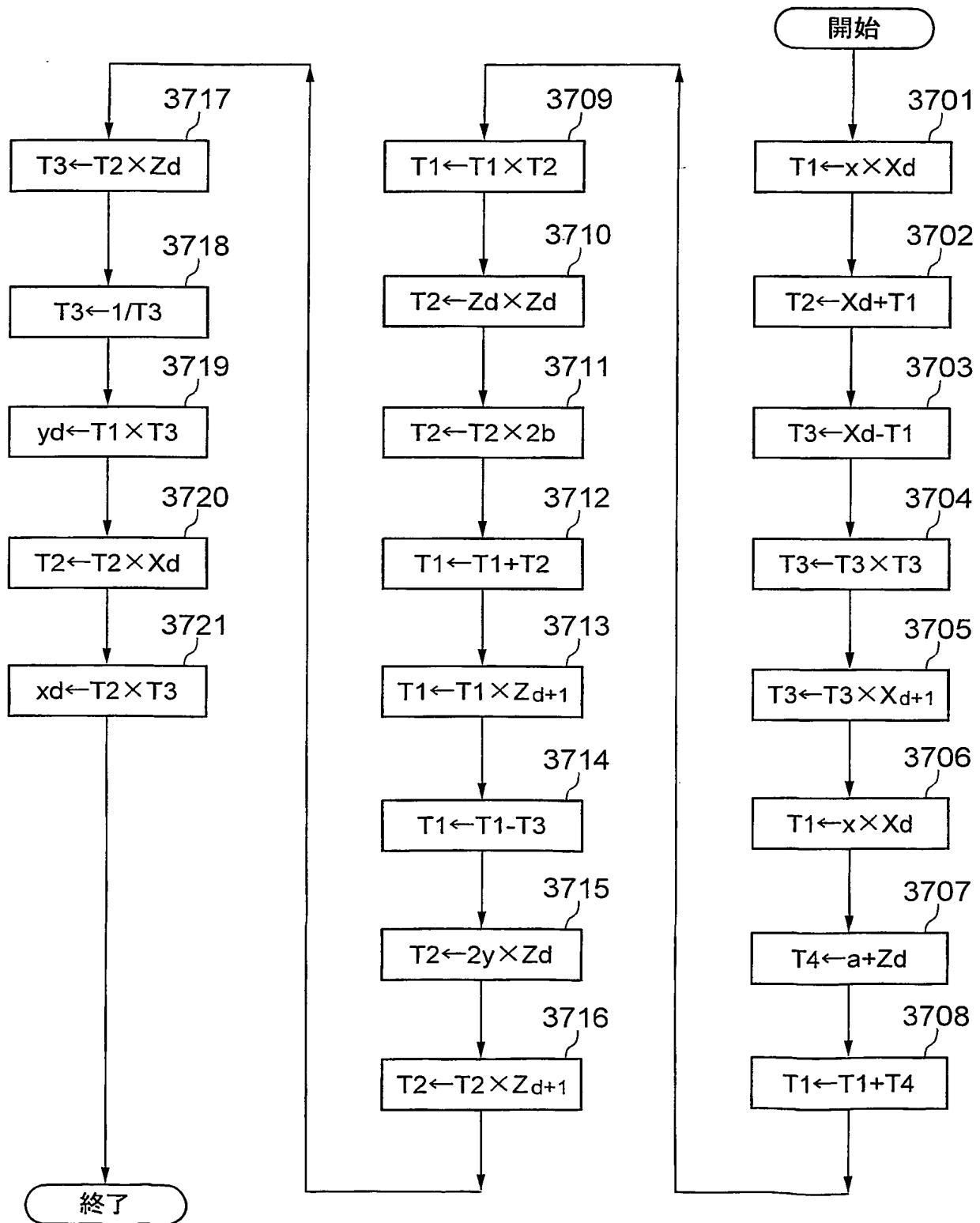
FIG. 36





37/45

FIG. 37





.

.

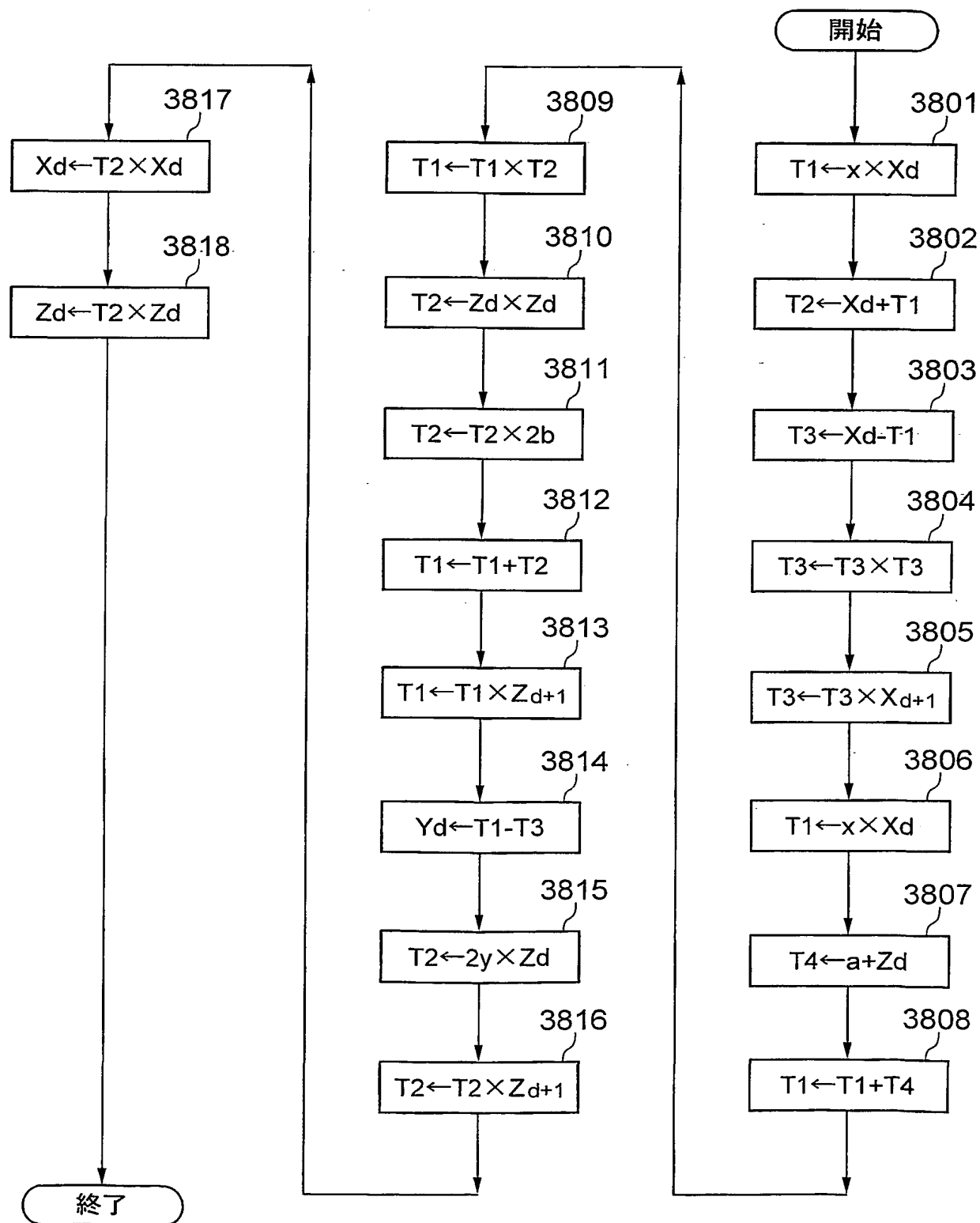
.

.

|

38/45

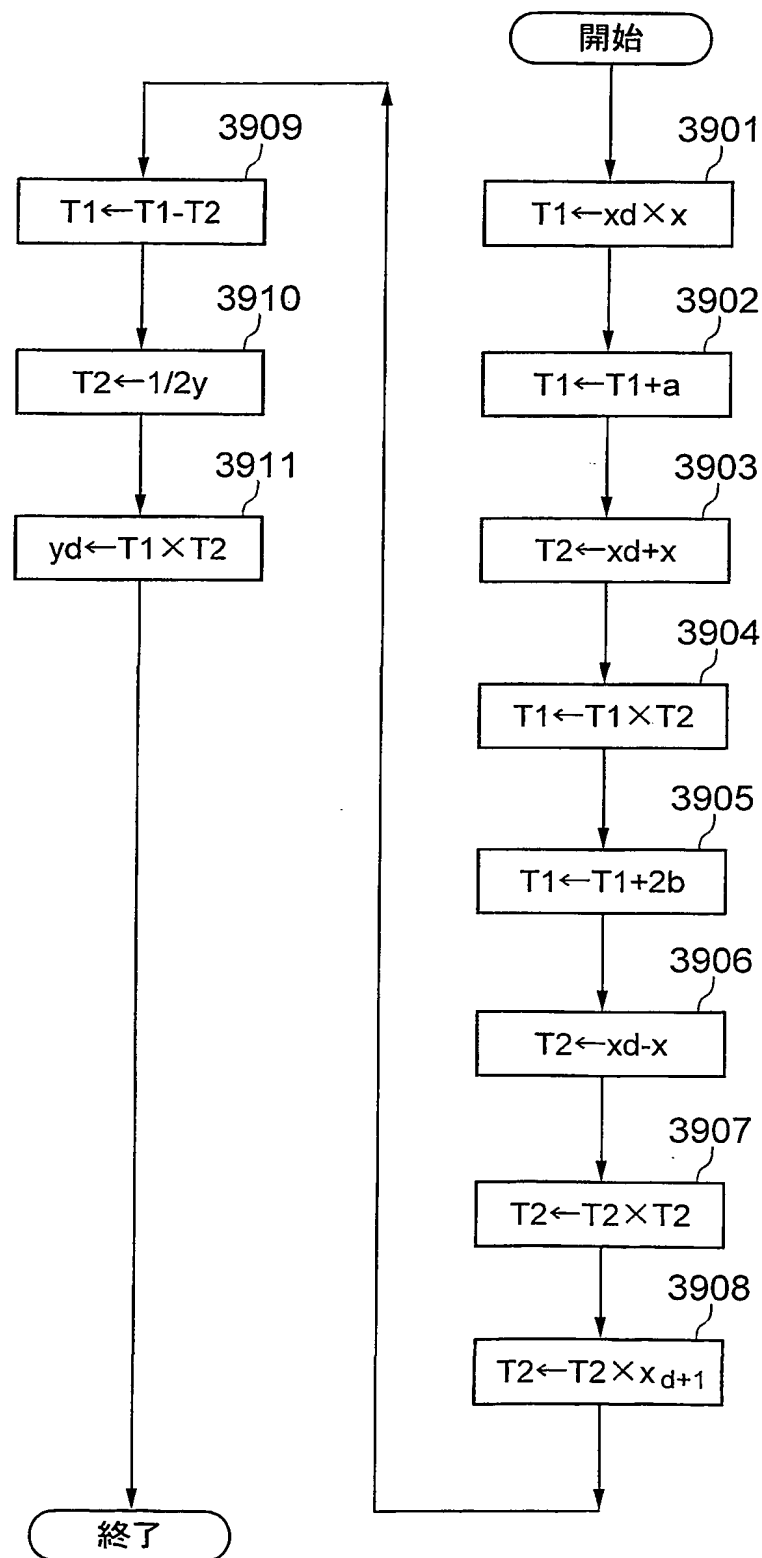
FIG. 38





39/45

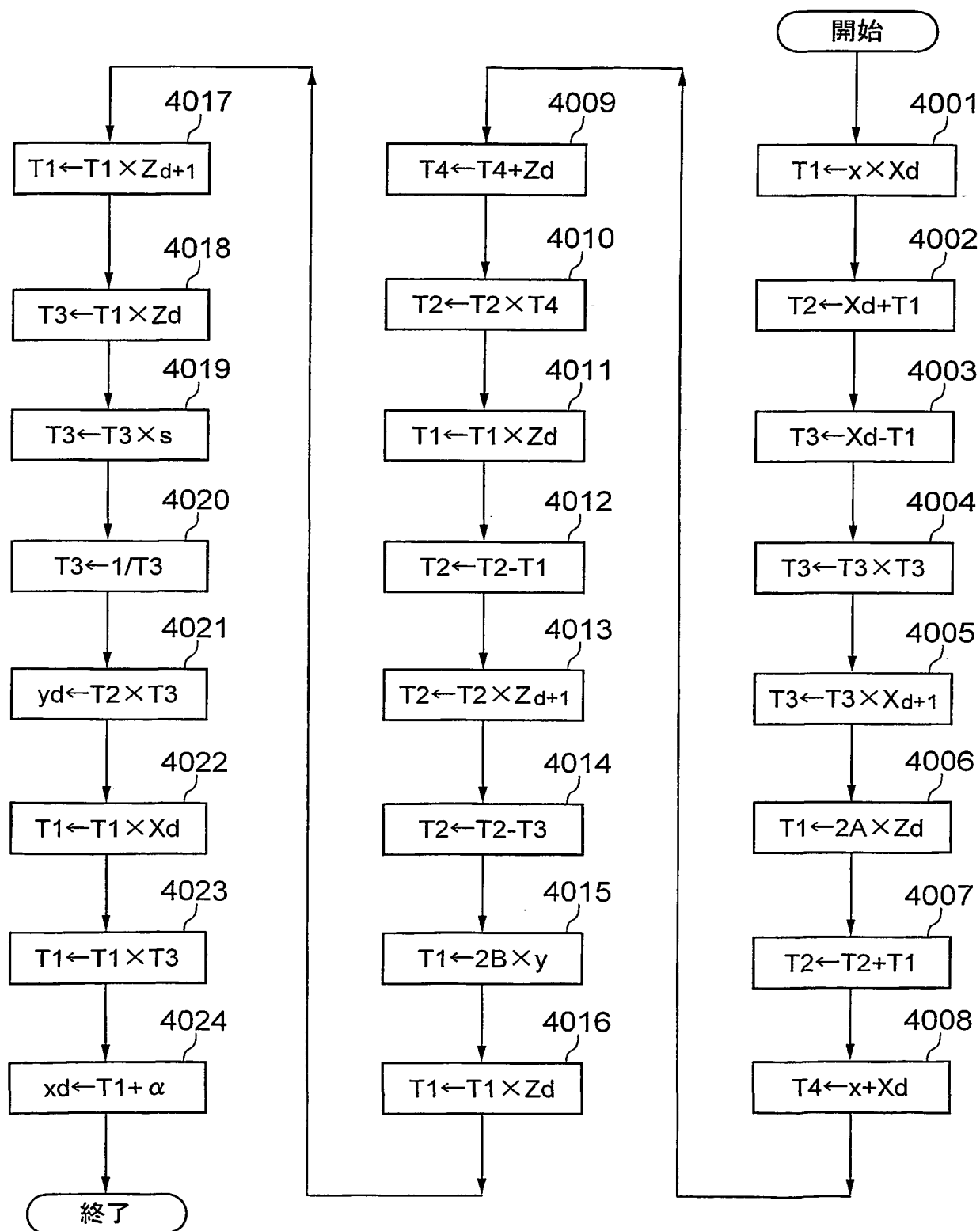
FIG. 39





40/45

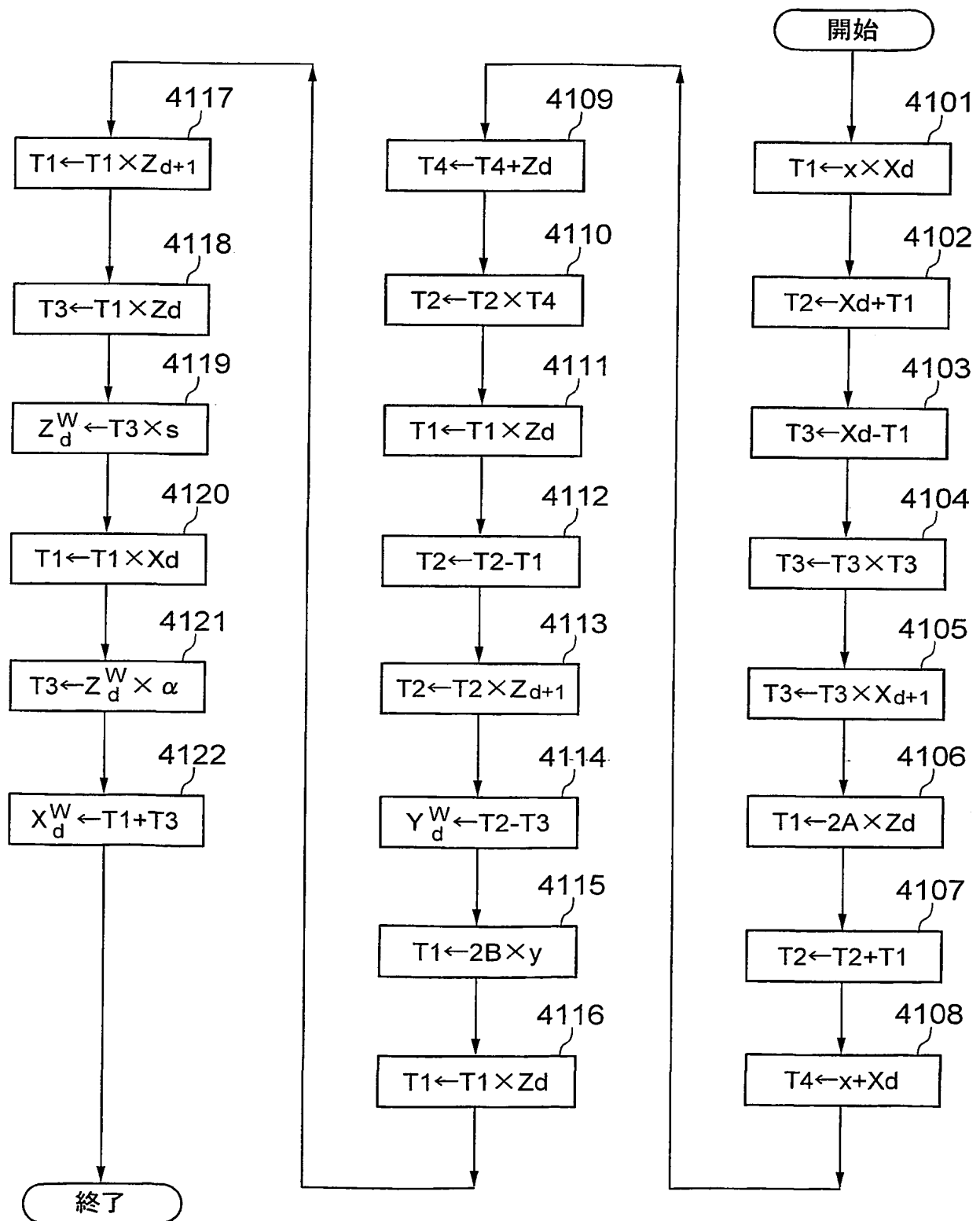
FIG. 40





41/45

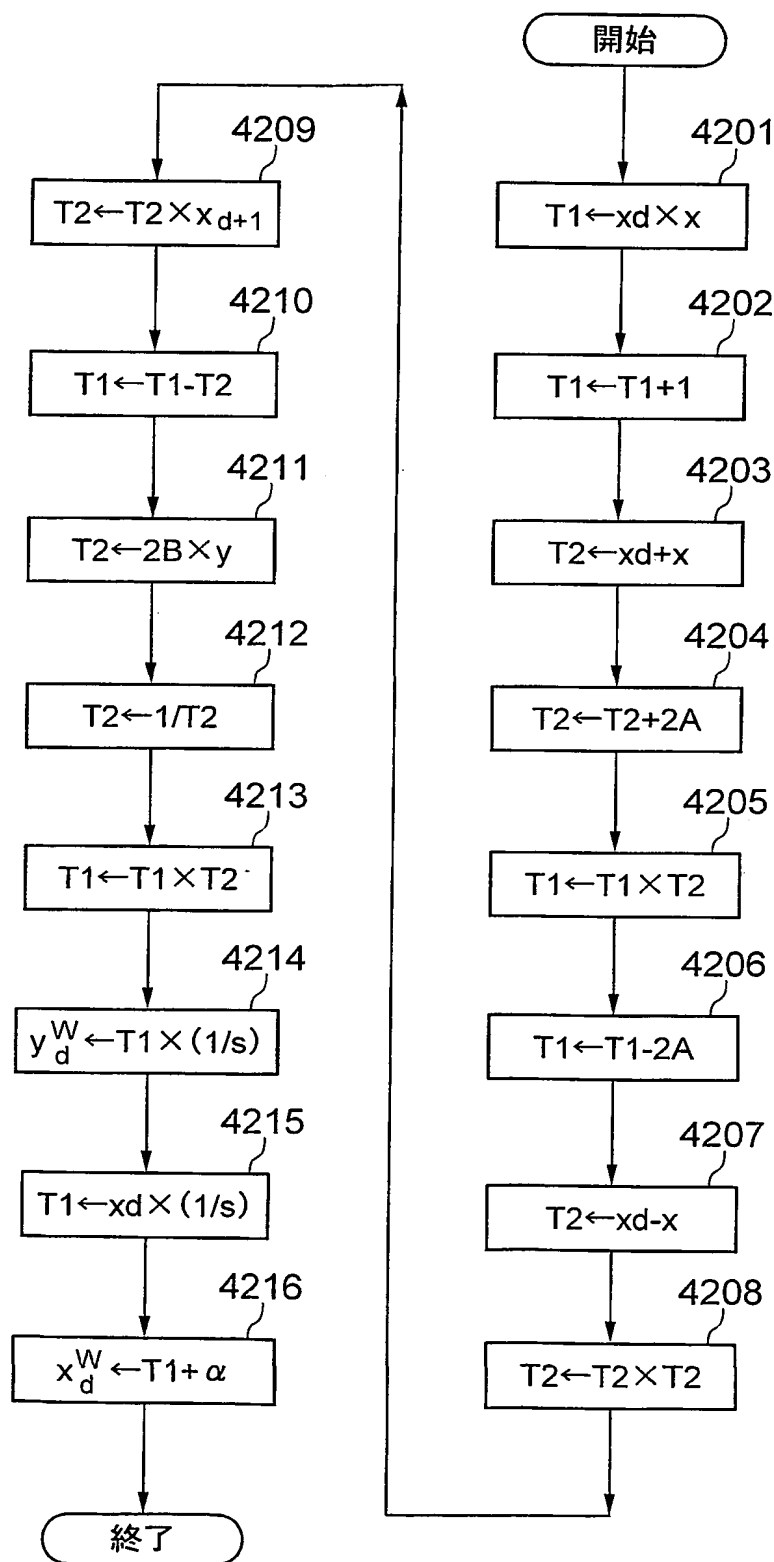
FIG. 41





42/45

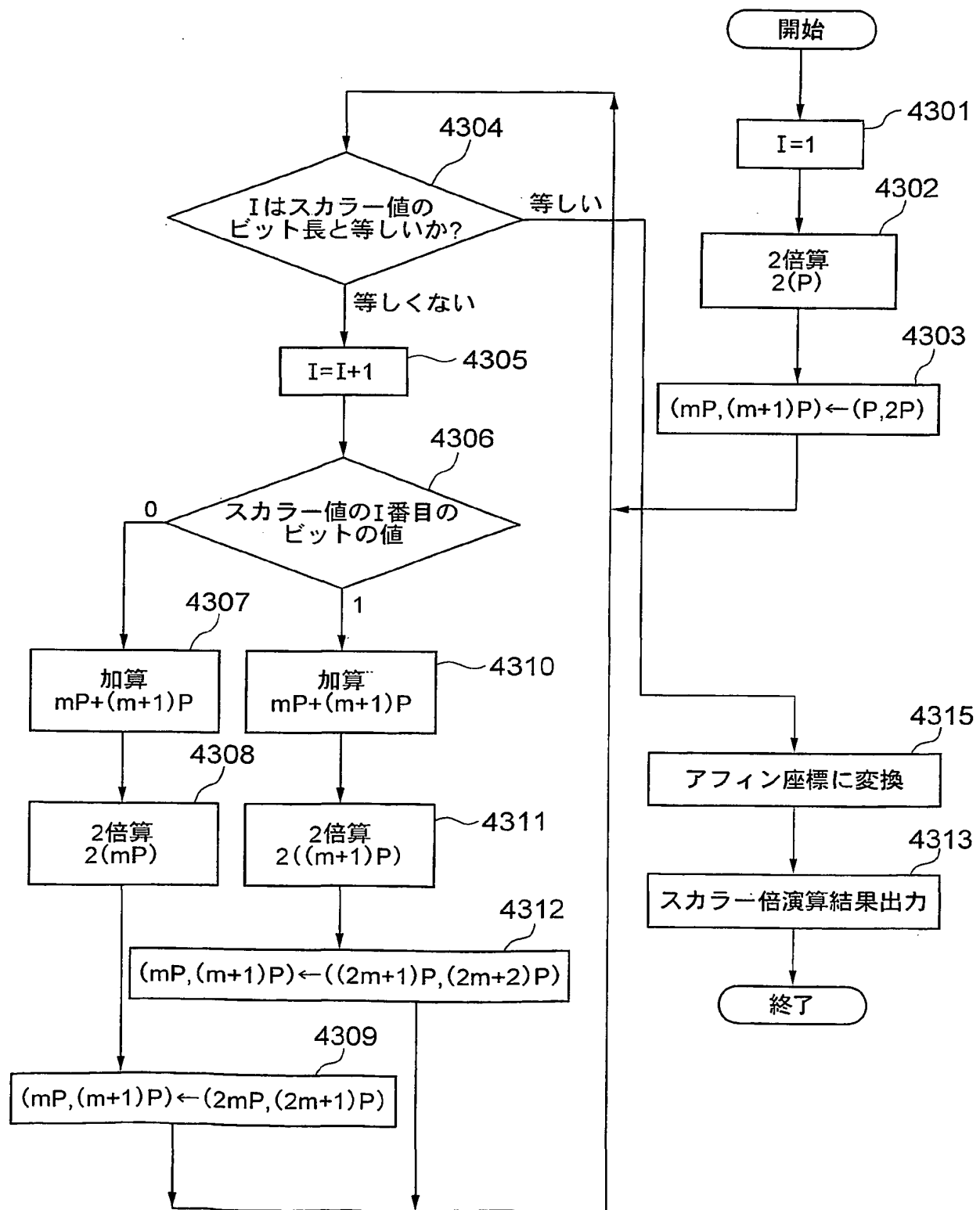
FIG. 42





43/45

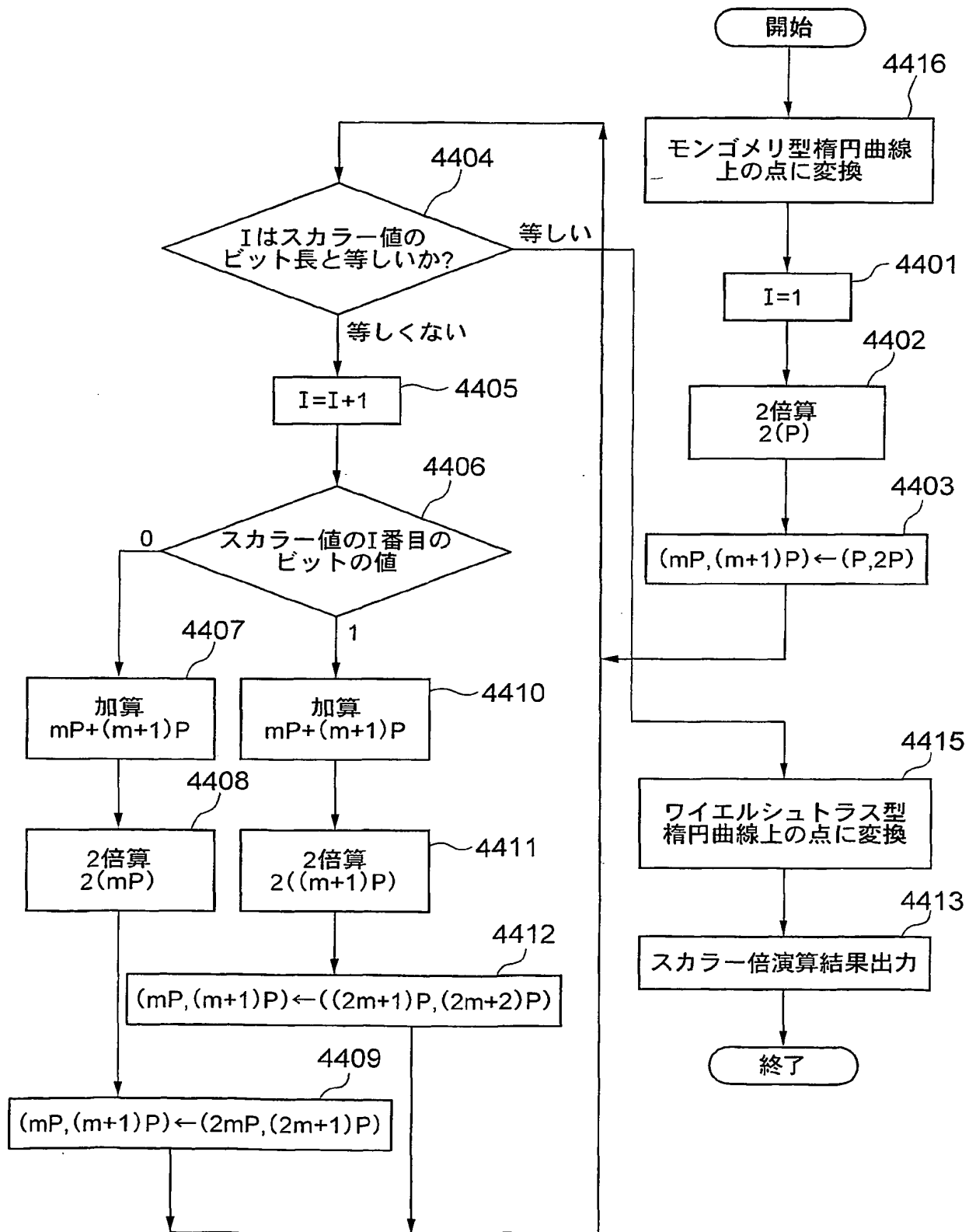
FIG. 43





44/45

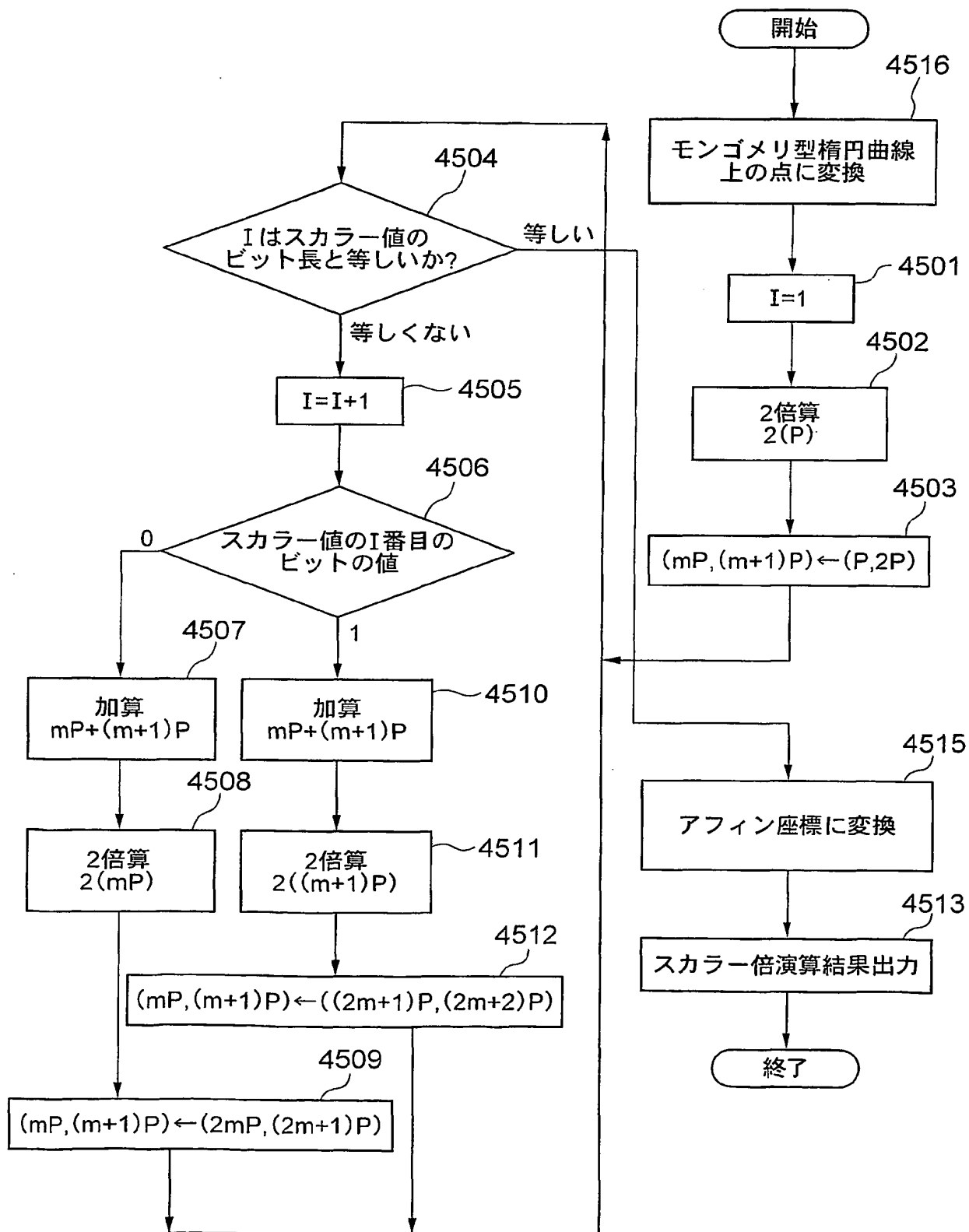
FIG. 44





45/45

FIG. 45





PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13ter.1(c) and 39)

Applicant's or agent's file reference E6369-00	IMPORTANT DECLARATION	Date of mailing (<i>day/month/year</i>) 11 December, 2001 (11.12.01)
International application No. PCT/JP01/09781	International filing date (<i>day/month/year</i>) 08 November, 2001 (08.11.01)	(Earliest) Priority Date (<i>day/month/year</i>) 08 November, 2000 (08.11.00)
International Patent Classification (IPC) or both national classification and IPC Int. Cl7 H04L9/30, G09C1/00		
Applicant Hitachi, Ltd.		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below.

1. ☒ The subject matter of the international application relates to:
 - a. ☐ scientific theories.
 - b. ☒ mathematical theories.
 - c. ☐ plant varieties.
 - d. ☐ animal varieties.
 - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
 - f. ☐ schemes, rules or methods of doing business.
 - g. ☐ schemes, rules or methods of performing purely mental acts.
 - h. ☐ schemes, rules or methods of playing games.
 - i. ☐ methods for treatment of the human body by surgery or therapy.
 - j. ☐ methods for treatment of the animal body by surgery or therapy.
 - k. ☐ diagnostic methods practised on the human or animal body.
 - l. ☐ mere presentations of information.
 - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art.
2. ☐ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:

☐ the description
 ☐ the claims
 ☐ the drawings
3. ☐ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:

☐ the written form has not been furnished or does not comply with the standard.
 ☐ the computer readable form has not been furnished or does not comply with the standard.
4. Further comments:

Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.



特 許 協 力 条 約

PCT

国際調査報告を作成しない旨の決定

(法第8条第2項、法施行規則第42条、第50条の3第
〔PCT17条(2)(a)、PCT規則13の3.1(c)、39〕

出願人又は代理人 の書類記号 E 6 3 6 9 - 0 0	重要決定	発送日 (日.月.年) 11.12.01
国際出願番号 PCT/JP01/09781	国際出願日 (日.月.年) 08.11.01	優先日 (日.月.年) 08.11.00
国際特許分類 (IPC) Int. Cl ⁷ H04L9/30, G09C1/00		
出願人 (氏名又は名称) 株式会社 日立製作所		

この出願については、法第8条第2項 (PCT17条(2)(a)) の規定に基づき、次の理由により国際調査報告を作成しない旨の決定をする。

- ☒ この国際出願は、次の事項を内容としている。
 - ☐ 科学の理論
 - ☒ 数学の理論
 - ☐ 植物の品種
 - ☐ 動物の品種
 - ☐ 植物及び動物の生産の本質的に生物学的な方法 (微生物学的方法による生産物及び微生物学的方法を除く。)
 - ☐ 事業活動に関する計画、法則又は方法
 - ☐ 純粋に精神的な行為の遂行に関する計画、法則又は方法
 - ☐ 遊戯に関する計画、法則又は方法
 - ☐ 人の身体の手術又は治療による処置方法
 - ☐ 動物の身体の手術又は治療による処置方法
 - ☐ 人又は動物の身体の診断方法
 - ☐ 情報の単なる提示
 - ☐ この国際調査機関が先行技術を調査できないコンピューター・プログラム
- ☐ この国際出願の次の部分が所定の要件を満たしていないので、有効な国際調査をすることができない。

<input type="checkbox"/> 明細書	<input type="checkbox"/> 請求の範囲	<input type="checkbox"/> 図面
------------------------------	--------------------------------	-----------------------------
- ☐ ナクレオチド又はアミノ酸の配列表が実施細則の附属書C (塩基配列又はアミノ酸配列を含む明細書等の作成のためのガイドライン) に定める基準を満たしていないので、有効な国際調査をすることができない。

<input type="checkbox"/> 書面による配列表が提出されていない又は所定の基準を満たしていない。
<input type="checkbox"/> フレキシブルディスクによる配列表が提出されていない又は所定の基準を満たしていない。
- 附記

名称及びあて名 日本国特許庁 (ISA/JP) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 中里 裕正	5M 9364
電話番号 03-3581-1101 内線 3597		





1/4

特許協力条約に基づく国際出願願書

原本（出願用） - 印刷日時 2001年11月08日 (08.11.2001) 木曜日 09時37分12秒

E6369-00

0	受理官庁記入欄	
0-1	国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	
0-4	様式-PCT/R0/101 この特許協力条約に基づく国際出願願書は、 右記によって作成された。	PCT-EASY Version 2.92 (updated 01.03.2001)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (R0/JP)
0-7	出願人又は代理人の書類記号	E6369-00
I	発明の名称	楕円曲線スカラー倍計算方法及び装置並びに記憶媒体
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除くすべての指定国 (all designated States except US)
II-4ja	名称	株式会社 日立製作所
II-4en	Name	HITACHI, LTD.
II-5ja	あて名:	101-8010 日本国 東京都 千代田区 神田駿河台四丁目6番地
II-5en	Address:	6, Kanda surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010 Japan
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名 (姓名)	桶屋 勝幸
III-1-4en	Name (LAST, First)	OKEYA, Katsuyuki
III-1-5ja	あて名:	244-0003 日本国 神奈川県 横浜市 戸塚区戸塚町5030番地
III-1-5en	Address:	株式会社 日立製作所 ソフトウェア事業部内 c/o Software Division, HITACHI, LTD. 5030, Totsukacho, Totsuka-ku, Yokohama-shi, Kanagawa 244-0003 Japan
III-1-6	国籍 (国名)	日本国 JP
III-1-7	住所 (国名)	日本国 JP

THIS PAGE BLANK (USPTO)

特許協力条約に基づく国際出願願書



原本（出願用） - 印刷日時 2001年11月08日 (08. 11. 2001) 木曜日 09時37分12秒

IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)
IV-1-1ja	氏名(姓名)	浅村 皓
IV-1-1en	Name (LAST, First)	ASAMURA, Kiyoshi
IV-1-2ja	あて名:	100-0004 日本国 東京都 千代田区 大手町2丁目2番1号 新大手町ビル331
IV-1-2en	Address:	Room 331, New Ohtemachi Bldg., 2-1, Ohtemachi 2-chome, Chiyoda-ku, Tokyo 100-0004 Japan
IV-1-3	電話番号	03-3211-3651
IV-1-4	ファクシミリ番号	03-3246-1239
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)
IV-2-1ja	氏名	浅村 肇
IV-2-1en	Name(s)	ASAMURA, Hajime
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR 及びヨーロッパ特許条約と特許協力条約の締約国 である他の国
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	US
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。	
V-6	指定の確認から除かれる国	なし (NONE)
VI-1	先の国内出願に基づく優先権主張	
VI-1-1	出願日	2000年11月08日 (08. 11. 2000)
VI-1-2	出願番号	特願2000-345457
VI-1-3	国名	日本国 JP
VI-2	先の国内出願に基づく優先権主張	
VI-2-1	出願日	2000年12月21日 (21. 12. 2000)
VI-2-2	出願番号	特願2000-393279
VI-2-3	国名	日本国 JP

THIS PAGE BLANK (USPTO)

特許協力条約に基づく国際出願願書

原本（出願用） - 印刷日時 2001年11月08日（08.11.2001）木曜日 09時37分12秒

VII-1	特定された国際調査機関 (ISA/A)	日本国特許庁 (ISA/JP)	
VIII	申立て	申立て数	
VIII-1	発明者の特定に関する申立て	-	
VIII-2	出願し及び特許を与えられる国際出願日における出願人の資格に関する申立て	-	
VIII-3	先の出願の優先権を主張する国際出願日における出願人の資格に関する申立て	-	
VIII-4	発明者である旨の申立て（米国を指定国とする場合）	-	
VIII-5	不利にならない開示又は新規性喪失の例外に関する申立て	-	
IX	照合欄	用紙の枚数	添付された電子データ
IX-1	願書（申立てを含む）	4	-
IX-2	明細書	156	-
IX-3	請求の範囲	9	-
IX-4	要約	1	e6369-00. txt
IX-5	図面	45	-
IX-7	合計	215	
	添付書類	添付	添付された電子データ
IX-8	手数料計算用紙	✓	-
IX-17	PCT-EASYディスク	-	フロッピーディスク
IX-18	その他	納付する手数料に相当する特許印紙を貼付した書面	-
IX-19	要約書とともに提示する図の番号	2	
IX-20	国際出願の使用言語名:	日本語	
X-1	提出者の記名押印		
X-1-1	氏名 (姓名)	浅村 皓	
X-2	提出者の記名押印		
X-2-1	氏名 (姓名)	浅村 肇	

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2	図面:	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP

THIS PAGE BLANK (USPTO)

特許協力条約に基づく国際出願願書

原本（出願用） - 印刷日時 2001年11月08日（08.11.2001）木曜日 09時37分12秒

10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	
------	----------------------------------	--

国際事務局記入欄

11-1	記録原本の受理の日	
------	-----------	--

THIS PAGE BLANK (USPTO)